(corresponding to US 6,026,293)

(11)

(19)日本国特許庁（ＪＰ）　(12)**公表特許公報（Ａ）**　(11)特許出願公表番号
特表2001－500293
（P2001－500293A）
(43)公表日　平成13年１月９日(2001.1.9)

| (51)Int.Cl.' | 識別記号 | ＦＩ | | ﾃｰﾏｺｰﾄﾞ(参考) |
|---|---|---|---|---|
| Ｇ０６Ｆ　12/14 | ３１０ | Ｇ０６Ｆ | 12/14 | ３１０Ｚ |
| Ｇ０９Ｃ　1/00 | ６４０ | Ｇ０９Ｃ | 1/00 | ６４０Ｄ |
| Ｈ０４Ｌ　9/32 | | Ｈ０４Ｂ | 7/26 | １０９Ｒ |
| Ｈ０４Ｑ　7/38 | | Ｈ０４Ｌ | 9/00 | ６７５Ａ |

審査請求　未請求　予備審査請求　有　（全 65 頁）

(21)出願番号　特願平10－512770
(86)(22)出願日　平成９年９月５日(1997.9.5)
(85)翻訳文提出日　平成11年３月５日(1999.3.5)
(86)国際出願番号　ＰＣＴ／ＵＳ９７／１５３１１
(87)国際公開番号　ＷＯ９８／１０６１１
(87)国際公開日　平成10年３月12日(1998.3.12)
(31)優先権主張番号　０８／７０６，５７４
(32)優先日　平成８年９月５日(1996.9.5)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　エリクソン　インコーポレイテッド
アメリカ合衆国27709　ノースカロライナ州，リサーチ　トライアングル　パーク，ピー．オー．ボックス　13969，ディベラップメント　ドライブ　7001
(72)発明者　オズボーン，ウィリアム，アール．
アメリカ合衆国27513　ノース　カロライナ州ケイリイ　ウェイク，ウォーターループステイション　ドライブ　107
(74)代理人　弁理士　浅村　皓　（外３名）

最終頁に続く

(54)【発明の名称】　電子メモリ改竄防止システム

(57)【要約】
セルラ電話のような電子装置内のメモリに対するいたずらを防止する方法及び装置が開示される。メモリ及び処理手段を有する電子装置が論理を含み、この論理は装置のメモリ内容に片方向ハッシュ計算を遂行するために使用され、それによって、このような内容の監査ハッシュ値、又はシグネチャが導出される。監査ハッシュ値は、真正メモリ内容から導出された認証された有効ハッシュ値と比較される。監査ハッシュ値と有効ハッシュ値との間の差がメモリいたずらの表示であり得る。本発明の他の態様に従って、電子装置メモリ内容を、そのメモリ内容にアクセスを許される前に認証されるデータ転送装置によって更新することができる。データ転送装置認証は、公衆／私用キー暗号化方式の使用に係わる。データ転送装置が電子装置とインタフェースしかつメモリ・アクセスをリクエストするとき、データ転送装置を認証するプロセスが開始される。

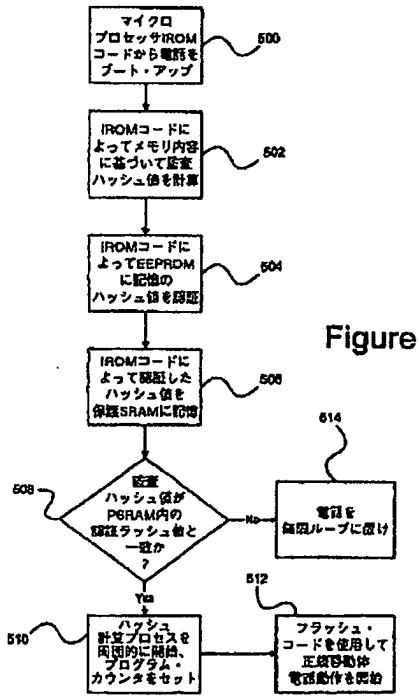



Figure 5

【特許請求の範囲】

１．　セルラ電話において、装置であって、

マイクロプロセッサと、

メモリと

を含み、

前記マイクロプロセッサが監査ハッシュ値を導出するために前記メモリの内容にハッシュ計算を遂行し、前記ハッシュ値が真正メモリ内容へのハッシュ計算の遂行から先に導出された有効ハッシュ値と比較される

装置。

２．　請求項１記載の装置において、前記監査ハッシュ値が周期的に導出されかつ前記有効ハッシュ値と比較される装置。

３．　請求項２記載の装置において、前記ハッシュ値の周期的導出がハードウェア・ベース・タイマの期限切れに従って遂行される装置。

４．　請求項１記載の装置において、前記メモリがフラシュ・メモリとＥＥＰＲＯＭとを含む装置。

５．　請求項１記載の装置であって、

保護されたランダム・アクセス・メモリ

を更に含み、前記ハッシュ計算が前記保護されたランダム・アクセス・メモリと連携して遂行される装置。

６．　請求項４記載の装置において、前記監査ハッシュ値がフラッシュ・メモリとＥＥＰＲＯＭの選択された内容に基づいて導出される装置。

７．　請求項６記載の装置において、前記選択された内容が電子直列番号を含む装置。

８．　請求項６記載の装置において、前記選択された内容がマイクロプロセッサ・プログラム・コードを含む装置。

９．　請求項１記載の装置において、前記有効ハッシュ値が前記メモリ内に記憶された公衆キーを使用して認証される装置。

１０．　請求項１記載の装置において、前記有効ハッシュ値が私用キーを使用

してディジタル・シグネチャを与えられる装置。

１１．　請求項１記載の装置において、前記ハッシュ計算がＳｎｅｒｆｕと、Ｈ－Ｈａｓｈと、ＭＤ２と、ＭＤ４と、ＭＤ５と、Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ（ＳＨＡ）と、ＨＡＶＡＬとから構成されるハッシュ関数の群から選択される装置。

１２．　請求項１０記載の装置において、ＥＬＧＡＭＡＬと、ＲＳＡと、ＤＳＡと、フィージ・フィアット・シャミアと、フィアット・シャミアとから構成されるアルゴリズムの群から選択される公衆／私用キー・システムが使用される装置。

１３．　請求項５記載の装置であって、安全論理を更に含み、前記安全論理が前記保護されたランダム・アクセス・メモリへのアクセスを監視する装置。

１４．　セルラ電話において、メモリいたずらを検出する方法であって、

メモリの選択された内容にハッシュ計算を遂行することによって発生された符号付き有効ハッシュ値を記憶するステップであって、前記選択されたメモリ内容が真正であると知られている前記記憶するステップと、

前記メモリの前記選択された内容に前記ハッシュ計算を遂行することによって監査ハッシュ値を発生するステップと、

前記監査ハッシュ値を前記有効ハッシュ値と比較するステップであって、それによって前記監査ハッシュ値と前記有効ハッシュ値との間の差が前記選択されたメモリ内容の変更を表示する前記比較するステップと

を含む方法。

１５．　請求項１４記載の方法において、前記監査ハッシュ値を前記発生するステップが保護されたランダム・アクセス・メモリと連携して遂行される方法。

１６．　請求項１４記載の方法であって、

私用キーに基づくディジタル・シグネチャで前記有効ハッシュ値を符号付けするステップ

を更に含む方法。

１７．　請求項１４記載の方法において、前記監査ハッシュ値を前記発生するステップと、前記監査ハッシュ値を前記有効ハッシュ値と前記比較するステップ

とが周期的に遂行される方法。

１８．　請求項１４記載の方法において、前記監査ハッシュ値を前記発生するステップがハードウェア・ベース・タイマの期限切れに従って遂行される方法。

１９．　請求項１４記載の方法において、前記監査ハッシュ値を前記発生するステップが監査ハッシュ値セグメントを計算することに係わる方法。

２０．　請求項１９記載の方法において、前記セルラ電話内に起こる他のプロセスが完了される間に監査ハッシュ値セグメントの計算を必要なだけ遅延させることができる方法。

２１．　請求項１４記載の方法において、前記有効ハッシュ値がディジタル・シグネチャを与えられ、及び前記監査ハッシュ値を前記有効ハッシュ値と前記比較するステップが前記シグネチャに対して前記有効ハッシュ値を認証するステップを含む方法。

２２．セルラ電話において、装置であって、

マイクロプロセッサと、

フラッシュ・メモリであって該メモリの内容が前記セルラ電話に対する動作命令を含む、前記フラッシュ・メモリと、

電気的消去可能プログラマブル読み出し専用メモリ（ＥＥＰＲＯＭ）であって、該ＥＥＰＲＯＭの内容が真正フラッシュ・メモリ内容の選択された部分とＥＥＰＲＯＭメモリ内容の選択された部分とに片方向ハッシュ計算を遂行することによって導出された有効ハッシュ値を含む前記ＥＥＰＲＯＭと

を含み、

前記マイクロプロセッサが前記選択された部分にハッシュ計算を遂行することによって監査ハッシュ値を周期的に発生し、前記フラッシュ・メモリと前記ＥＥＰＲＯＭメモリの少なくとも１つが変更されたかどうか評定するために前記監査ハッシュ値が前記認証された有効ハッシュ値と比較される

装置。

２３．　請求項２２記載の装置において、片方向ハッシュ計算がＳｎｅｒｆｕと、Ｈ－Ｈａｓｈと、ＭＤ２と、ＭＤ４と、ＭＤ５と、Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ（ＳＨＡ）と、ＨＡＶＡＬとから構成される群から選択さ

れ

る装置。

２４．　請求項２２記載の装置において、前記監査ハッシュ値が記憶されるのに先立ち私用キーによるディジタル・シグネチャを受け取り、かつ前記監査ハッシュ値との比較目的のために公衆キーによって認証される装置。

２５．　請求項２４記載の装置において、使用される公衆／私用キー・システムがＥＬＧＡＭＡＬと、ＲＳＡと、ＤＳＡと、フィージ・フィアット・シャミアと、フィアット・シャミアとから構成されるアルゴリズムの群から選択される装置。

２６．　請求項２４記載の装置において、前記監査ハッシュ値が前記セルラ電話の外部の処理手段を使用して前記私用キーによるディジタル・シグネチャを受け取る装置。

２７．　セルラ電話をプログラムするシステムであって、

データ転送装置

を含み、

前記セルラ電話が前記データ転送装置から受信したアクセス・リクエスト・メッセージに応答して呼び掛け応答認証プロセスを開始する

システム。

２８．　セルラ電話メモリ・プログラミング能力への無許可アクセスを防止するシステムであって、

セルラ電話であって、

データを記憶するメモリと、

公衆キー認証用手段を有するマイクロプロセッサと

を含む前記セルラ電話と、

前記セルラ移動体電話へ符号付きメッセージを供給するために私用キー・ディジタル・シグネチャ手段を有するマイクロプロセッサを含むデータ転送装置であって、前記私用キー・シグネチャ手段が公衆キー認証手段に対応する前記データ転送装置と

を含み、

前記セルラ電話マイクロプロセッサが前記データ転送装置によって供給された

符号付きメッセージの分析に基づいて前記データ転送装置の真正を評定する
システム。

２９．　セルラ電話プログラミング装置の真正を評定する方法であって、

プログラミング・リクエストに応答して呼び掛けメッセージを送るステップと

、

私用暗号化キーを使用してデータ転送装置内で前記呼び掛けメッセージを符号付けするステップと、

前記セルラ電話に前記符号付け呼び掛けメッセージを送るステップと、

公衆キーの使用によって前記セルラ電話内の前記符号付きメッセージを認証するステップであって、前記公衆キーが前記私用暗号化キーに対応する前記認証するステップと、

もし前記呼び掛けメッセージが前記認証するステップによって回復されないならば前記データ転送装置を拒否するステップと
を含む方法。

３０．　セルラ電話をプログラムするためにデータ転送装置を含むシステムにおいて、前記セルラ電話内メモリへの無許可アクセスを防止する方法であって、

前記データ転送装置から前記セルラ電話へプログラミング・リクエストを送るステップと、

前記転送リクエストに応答して、前記セルラ電話から前記データ転送装置へ呼び掛けメッセージを送るステップと、

私用キーを使用して前記データ転送装置内の呼び掛け応答メッセージを符号付けするステップであって、前記呼び掛け応答メッセージが前記呼び掛けメッセージの部分に依存する前記符号付けするステップと、

前記セルラ電話へ前記符号付き呼び掛け応答メッセージを送るステップと、

前記私用キーに対応する公衆キーの使用によって前記セルラ電話内の前記呼び掛け応答メッセージを認証するステップと、

もし前記符号付き呼び掛け応答メッセージの認証が前記データ転送装置の真正を確認するならばプログラミング・モードに入るステップと
を含む方法。

３１．　セルラ電話をプログラムするシステムであって、

プログラマと、
第１ポートと第２ポートとを有する汎用コンピュータと
を含み、
前記プログラマが前記第１ポートに取付け可能であり、かつ前記第２ポートがプログラムされるセルラ電話とインタフェースするために使用され、前記プログラマから受信された前記セルラ電話をプログラムするリクエストに応答して、前記セルラ電話が呼び掛けを返し、前記呼び掛けが前記プログラマによって符号付けされかつ認証のために前記セルラ電話に返され、それによって前記符号付き呼び掛けの認証を通しての前記呼び掛けの回復がプログラマ真正を表示しかつ前記セルラ電話をプログラミング・モードに入れさせる
システム。

３２．　セルラ電話において、装置であって、
マイクロプロセッサ
を含み、
プログラマから受信された前記セルラ電話をプログラムするリクエストに応答して、前記セルラ電話内の前記マイクロプロセッサが前記プログラマへ呼び掛けを発し、前記呼び掛けが前記プログラマによって符号付けされかつ認証のために前記セルラ電話に返され、それによって前記符号付き呼び掛けの適正認証がプログラマ真正を表示しかつ前記セルラ電話をプログラミング・モードに入れさせる装置。

３３．　セルラ電話において、詐欺メモリ・アクセスを防止するシステムであって、
安全論理と、
命令コードを含む読み出し専用メモリと、

保護されたランダム・アクセス・メモリと

を含み、

前記安全論理が前記読み出し専用メモリ以外の素子による前記保護されたランダム・アクセス・メモリへのアクセスを防止する

システム。

３４．　請求項３３記載のシステムであって、ハードウェア・ベース・タイマを更に含み、前記安全論理が前記読み出し専用メモリ以外の素子による前記ハードウェア・ベース・タイマへのアクセスを防止するシステム。

３５．　請求項３３記載のシステムにおいて、前記読み出し専用メモリ内の命令コードに従う前記保護されたランダム・アクセス・メモリへのアクセスは、前記システムが監視モードにあるときに限り起こり得るシステム。

３６．　電子装置において、装置であって、

マイクロプロセッサと、

メモリと

を含み、

前記マイクロプロセッサが監査ハッシュ値を導出するために前記メモリの内容にハッシュ計算を遂行し、前記ハッシュ値が真正メモリ内容へのハッシュ計算の遂行から先に導出された有効ハッシュ値と比較される

装置。

３７．　請求項３６記載の装置において、前記監査ハッシュ値が周期的に導出されかつ前記有効ハッシュ値と比較される装置。

３８．　請求項３６記載の装置において、前記メモリがフラシュ・メモリとＥＰＲＯＭとを含む装置。

３９．　請求項３６記載の装置において、前記監査ハッシュ値がフラッシュ・メモリとＥＥＰＲＯＭの選択された内容に基づいて導出される装置。

４０．　請求項３７記載の装置において、前記選択された内容がマイクロプロセッサ・プログラム・コードを含む装置。

４１．　請求項３６記載の装置において、前記有効ハッシュ値が前記メモリ内

に記憶された公衆キーを使用して認証される装置。

４２．　請求項３６記載の装置において、前記遂行されたハッシュ計算が私用キーを使用してディジタル・シグネチャを与えられる装置。

４３．　請求項３６記載の装置において、前記有効ハッシュ値がＳｎｅｒｆｕと、Ｈ－Ｈａｓｈと、ＭＤ２と、ＭＤ４と、ＭＤ５と、Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ（ＳＨＡ）と、ＨＡＶＡＬとから構成されるハッシュ関数の

群から選択される装置。

４４．　請求項４２記載の装置において、使用される公衆／私用キー・システムがＥＬＧＡＭＡＬと、ＲＳＡと、ＤＳＡと、フィージ・フィアット・シャミアと、フィアット・シャミアとから構成される公衆キー・アルゴリズムの群から選択される装置。

４５．　電子装置において、メモリいたずらを検出する方法であって、

メモリの選択された内容にハッシュ計算を遂行することによって発生された符号付き有効ハッシュ値を記憶するステップであって、前記選択されたメモリ内容が真正であると知られている前記記憶するステップと、

前記メモリの前記選択された内容に前記ハッシュ計算を遂行することによって監査ハッシュ値を発生するステップと、

前記監査ハッシュ値を前記有効ハッシュ値と比較するステップであって、それによって前記監査ハッシュ値と前記有効ハッシュ値との間の差が前記選択されたメモリ内容の変更を表示する前記比較するステップと

を含む方法。

４６．　請求項４５記載の方法であって、私用キーに基づくディジタル・シグネチャで前記有効ハッシュ値を符号付けするステップを更に含む方法。

４７．　請求項４５記載の方法において、前記監査ハッシュ値を前記発生するステップと、前記監査ハッシュ値を前記有効ハッシュ値と前記比較するステップとが周期的に遂行される方法。

４８．　請求項４５記載の方法において、前記監査ハッシュ値を前記発生する

ステップが監査ハッシュ値セグメントを計算することに係わる方法。

４９．　請求項４８記載の方法において、前記電子装置内に起こる他のプロセスが完了される間に監査ハッシュ値セグメントの計算を必要なだけ遅延させることができる方法。

５０．　請求項４５記載の方法において、前記有効ハッシュ値がディジタル・シグネチャを与えられ、及び前記監査ハッシュ値を前記有効ハッシュ値と前記比較するステップが前記シグネチャに対して前記有効ハッシュ値を認証するステップを含む方法。

５１．　電子装置をプログラムするシステムであって、

データ転送装置

を含み、

前記電子装置が前記データ転送装置から受信したアクセス・リクエスト・メッセージに応答して呼び掛け応答認証プロセスを開始する

システム。

５２．　詐欺メモリ・アクセスを防止するシステムであって、

安全論理と、

命令コードを含む読み出し専用メモリと、

保護されたランダム・アクセス・メモリと

を含み、

前記安全論理が前記読み出し専用メモリ以外の素子による前記保護されたランダム・アクセス・メモリへのアクセスを防止する

システム。

５３．　請求項５２記載のシステムであって、ハードウェア・ベース・タイマを更に含み、前記安全論理が前記読み出し専用メモリ以外の素子による前記ハードウェア・ベース・タイマへのアクセスを防止するシステム。

５４．　請求項５２記載のシステムにおいて、前記読み出し専用メモリ内の命令コードに従う前記保護されたランダム・アクセス・メモリへのアクセスは、前記システムが監視モードにあるときに限り起こり得るシステム。

【発明の詳細な説明】

# 電子メモリ改竄防止システム

## 背　景

本発明は、電子メモリ操作、特に、電子装置内の安全が望まれるメモリ内容の無許可操作を防止する方法及び装置に関する。

本明細書に開示される発明は、安全な又は好適には不変の状態に維持されるべきメモリ内容を有するあらゆる電子装置に関する。このような要件は、セルラ電話メモリの詐欺（ｆｒａｕｄｕｌｅｎｔ）操作を防止するような安全理由によって、又は航空機制御又は医療機器動作のような臨界応用での電子装置動作の保全性を維持する目的のために必要とされると云ってよい。本明細書に開示しかつ説明するように、本発明の模範的態様を、セルラ電話内の１つ以上の電子メモリの安全を保証するシステム及び方法についての説明の中で述べる。本明細書でまた説明するのは、電子メモリにアクセスすることを許される前に認証プロセスを受けるデータ転送装置を使用することによって、電子装置内の１つ以上の電子メモリへのアクセス及びメモリの操作を許すシステムである。後者のシステムもまた、セルラ電話応用についての説明の中で述べる。たとえ本明細書に開示された本発明の模範的実施例を安全セルラ電話メモリ及びセルラ電話内のメモリ内容を安全にアクセスし及び変更する手段についての説明の中で述べたとしても、当業者が容易に承知するように、本発明に従うシステムは、その内容が不変に維持されるべき又はその内容が許可された手段によってのみアクセスされるべき１つ以上のメモリを有するあらゆる電子システムに応用することができる。したがって、本発明の範囲を、本明細書で扱う模範的実施例によって限定するのではなく、本明細書に添付された請求の範囲及びそれの等価事項によって限定することを意図する。

米国では、セルラ電話詐欺に因る損失が１９９５年に６億ドルと見積もられた。これに反応して、製造業者、サービス提供業者、連邦通信委員会（Ｆｅｄｅｒａｌ　Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｃｏｍｍｉｓｓｉｏｎ；

ＦＣＣ）及び業界取り引き団体がこのような詐欺と戦ういくつもの技術を調査し

てきている。米国で行われたセルラ電話詐欺の大部分は、セルラ電話が通信を確立するために備えなければならないセルラ電話の電子直列番号（ｅｌｅｃｔｒｏｎｉｃ　ｓｅｒｉａｌ　ｎｕｍｂｅｒ；ＥＳＮ）を変更するメモリ操作のいくつかの手口に係わる。したがって、ＦＣＣによる規則としての考えの下で、１つの詐欺防止技術は、セルラ電話製造業者に、全てのマイクロプロセッサ・コード及びＥＳＮを変更不可能にするように要求することである。本発明を組み込むシステムが取り組むセルラ電気通信動作環境及び関連した問題を解説するに当たって助けとなるために基本的セルラ通信について或る背景を下に与える。

セルラ通信システムの簡単化レイアウトを図１に示す。移動体電話Ｍ１～Ｍ１０がセルラ基地局Ｂ１～Ｂ１０と無線信号を受信することによって公衆交換網（ｐｕｂｌｉｃ　ｓｗｉｔｃｈｅｄ　ｎｅｔｗｏｒｋ）の固定部分と通信する。セルラ基地局Ｂ１～Ｂ２は、移動交換センタ（Ｍｏｂｉｌｅ　Ｓｗｉｔｃｈｉｎｇ　Ｃｅｎｔｅｒ；ＭＳＣ）を経由して公衆交換網と接続される。各基地局Ｂ１～Ｂ１０は、相当する領域、つまり、「セル」Ｃ１～Ｃ１０内に信号を送信する。図１に示したように、基地局の理想的な配置は、それらのセルが、重なり合う量を最小限にして、移動電話通信が普通その中で起こるエリア（例えば、都市エリア）を実質的にカバーするように組織される。

利用者が或る１つのセル内で移動体電話を起動させると、移動体電話はその移動体電話の存在を表示する信号をそのセルの基地局へ送信する。移動体電話は、各基地局によって連続的に監視されている指定されたセットアップ・チャネルに、その移動体電話のＥＳＮを含むことがある信号を送信する。基地局が移動体電話の信号を受信すると、基地局はそのセル内の移動体電話の存在を登録する。このプロセスは、移動体電話が他のセル内へ移動する際にそれが適当に登録されるように、連続的に繰り返される。

移動体電話番号がダイヤルされると、電話会社の電話局がその番号を移動体電話として認識しかつその呼をＭＳＣへ転送する。MSCは、ダイヤルされた移動体電話番号及び現在登録情報に基づいて或る決まったいくつかの基地局へページング・メッセージを送る。これらの基地局の１つ以上がそのセットアップ・チャ

ネル上でページを送信する。ダイヤルされた移動体電話は、セットアップ・チャネル上のその識別情報を認識し、かつ基地局ページに応答する。移動体電話はまた、割り当てられた音声チャネルに同調するようにとの命令に従い、次いで呼び出し信号を開始する。移動体利用者が通信を終端させるとき、信号確認音が基地局へ送信され、両側が音声チャネルを解放する。

上に述べた動作で、移動体電話は固定網に持久的に接続されないで、代わりに、いわゆる「エア・インタフェース（ａｉｒ　ｉｎｔｅｒｆａｃｅ）」を通して基地局と通信する。これは、もちろん、利用者が通信システムに物理的にリンクされる制約を伴わずに容易に移動体電話を輸送することができるから、セルラ通信システムの柔軟性を与える。しかしながら、この同じ特徴がまた、セルラ電話システムを通じて送信される情報の安全を保証することに関して困難を生じる。

例えば、普通の有線電話システムでは、電話局交換機は、電話機が物理的に付属している通信線路によるその電話機の使用について課金される特定加入者を識別することができる。それゆえ、加入者の勘定を詐欺により使用するには、典型的に、その加入者線路へ物理的接続を行うことを必要とする。これが、詐欺をたくらむ利用者に発見の危険を存在させる。

他方、セルラ電気通信システムはエア・インタフェースを通じて通信するから、これらのシステムは詐欺をたくらむ利用者にこのような接続問題を課さない。保護システムが欠如しているので、詐欺による利用者は、通信を確立しかつ維持するために種々の時間に移動体電話によって網へ送信される他の加入者の電子シリアル番号（ＥＳＮ）にアクセスすることによってその加入者の勘定を使用することができる。

標準セルラ接続を確立するに当たって、２つの識別コードが移動体電話によってシステムへ送信される。これらは、移動体識別番号（Ｍｏｂｉｌｅ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ；ＭＩＮ）及びＥＳＮである。ＭＩＮは、加入者を識別するのに対して、ＥＳＮはその加入者によって使用される実際ハードウェアを識別する。したがって、加入者が新機器を購入することによって、特定ＥＳＮに対応するＭＩＮは、時間が経つにつれて変化し得ると予想

される。ＭＩＮが１０桁の登録簿（ｄｉｒｅｃｔｏｒｙ）電話番号であるのに対して、ＥＳＮは移動体電話を固有的に識別する３２ビット２進番号である。ＥＳＮは、典型的に、移動体電話製造業者によってセットされる。

例えば、アドバンスト・モビール・ホーン・システム（Ａｄｖａｎｃｅｄ Ｍｏｂｉｌｅ Ｐｈｏｎｅ Ｓｙｓｔｅｍ；ＡＭＰＳ）で通信を設定する（ｓｅｔｔｉｎｇ ｕｐ）に当たって利用される慣例の認証方法は、図２に描いた流れ図によって示される。この方法に従って、ブロック２００で、基地局は、移動体電話からのＥＳＮ及びＭＩＮの両方を受信する。これらの認証コードは、これが移動体電話から受信されることを表示するために、$ESN_m$及び$MIN_m$で指定される。次に、ブロック２０２で、基地局は、システム・メモリから$MIN_m$に対応する$ESN_{sys}$を検索する。次いで、ブロック２０４で、$ESN_{sys}$が$ESN_m$と比較される。もしこれら２つのシリアル番号が同じであるならば、流れ図はブロック２０６へ進み、かつシステム・アクセスが許される。そうでなければ、システム・アクセスは、ブロック２０８で否定される。

このシステムの１つの欠点は、エア・インタフェース上で又は他の発信源から盗聴することによって、有効ＭＩＮ／ＥＳＮを組み合わせることが詐欺による利用者にとって比較的簡単であることである。もし移動体電話から受信されたＭＩＮ及びＥＳＮがシステム・メモリに記憶されたものに相当するならば、この従来のシステムによるアクセスは有効であると推定されるから、詐欺アクセスにとって必要な情報の全ては、電子盗聴によって得ることができる。

欧州ＧＳＭ規格（移動体通信用グローバル・システム（Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎ；ＧＳＭ））、来国ＴＩＡ／ＥＩＡ／ＩＳ－１３６、及び日本パーソナル・ディジタル・セルラ規格無線通信システムの下で動作するシステムでは、盗聴から生じる詐欺は呼び掛け応答（ｃｈａｌｌｅｎｇｅ－ｒｅｓｐｏｎｓｅ）方法によって防止される。呼び掛け応答方法に従って、各移動体電話は、その移動体電話及び網内のデータベースの両方に記憶されている固有の秘密キーと関連している。システムに固有であるアルゴリズムが各移動体電話及び所望の網ノードに記憶される。呼が設定されると、認証がリクエストされ、それによって網が呼び掛け（乱数）

を移動体電話へ送る。受信した呼び掛け及び記憶した秘密キーに基づいて、移動体電話は、そのアルゴリズムを使用して応答を計算し、その応答を網へ送信する。同時に、網は「同じ呼び掛け及び網記憶秘密キーに基づいて「期待」応答を計算する。次いで、網は移動体電話の計算した応答を受信し、移動体電話の計算した応答を網の計算した応答と比較する。もし不一致が起こるならば、適当な行動を取ることになる、例えば、アクセスが否定されるか又は警告フラグがセットされる。移動無線システムで基地局と移動体電話との間で認証検査を実施する方法は、ｐ・デント（Ｐ．Ｄｅｎｔ）他の米国特許第５，２８２，２５０号に記載されている。

ＡＭＰＳのような、慣例のアナログ・システムでは、ほとんどの詐欺が、有効ＭＩＮ／ＥＳＮ対を獲得しかつセルラ電話をリプロルグラムするためにこの対を使用することによって有効加入者を「偽造（ｃｌｏｎｅ）」する詐欺による利用者によって行なわれる。もっと精巧な偽造の構成では、セルラ電話のソフトウェアがいくつかのＭＩＮ／ＥＳＮ対を「タンブリング（ｔａｍｂｌｉｎｇ）」と呼ばれる実践に使用することができるように、このソフトウェアがリプログラムされる。タンブリング・ルーチンを用いてプログラムされたセルラ電話は、呼を開始するために、ランダムにスクロールしてＭＩＮ／ＥＳＮ対を選択する。サービス提供業者又は加入者によって詐欺が識別されるにつれて、そのＭＩＮ／ＥＳＮ対は無効とされる。発呼を企図しているとき無効ＭＩＮ／ＥＳＮ対に遭遇すると、タンブリング・ルーチンは、単にそのＭＩＮ／ＥＳＮ対を取り消しかつ有効ＭＩＮ／ＥＳＮ対が発見されるまでスクローリングを続ける。セルラ電話内へプログラムされたこのＭＩＮ／ＥＳＮ対の全てが無効化された後、電話利用者は典型的に、そのセルラ電話内へプログラムされたＭＩＮ／ＥＳＮ対の新しい組を有するように偽造者（ｃｌｏｎｅｒ）に報いる。

ほとんどのセルラ詐欺は、成る程度のメモリ操作に係わる。これを図３を参照して説明するが、この図は従来のセルラ電話メモリ及びプロセッサ構成を示す。コントローラ３００が、メモリ・バス３０８を使用して、ＲＯＭ又はフラッシュ・メモリ３２０、ＥＥＰＲＯＭ３１０、及びランダム・アクセス・メモリ（ＲＡＭ）３３０と通信する。プログラムラ・メモリ３２０は不揮発性読み出し書き込

みメモリであり、これはセルラ電話の全般動作に使用されるコードの大部分を記憶するために使用される。ＥＥＰＲＯＭ３１０はＭＩＮ／ＥＳＮ対３１４と３１６、及び利用者プロファイル情報３１２（例えば、スピード・ダイヤリング番号）を記憶するために使用され、及びＲＡＭは読み出し書き込みスクラッチパッドに使用される。偽造者は、使用する情報を収集するためにメモリとコントローラ３００との間でメッセージを監視し、フラッシュ・メモリ３２０又はＥＥＰＲＯＭ３１０に記憶された情報を迂回する又は改変することを知っている。

電話詐欺の最も普通の方法は、ＥＳＮを変えるための、電話サービスや修繕を意図する試験命令の不法使用であった。しかしながら、より最近開発された電話はこのようないたずらには対抗性があって、この手の攻撃を有効に除去している。したがって、偽造者は、より精巧な方法による攻撃に訴えてきた。

１つのこのようなテクニックは、ＥＳＮ３１４を含む元のＥＥＰＲＯＭ３１０を除去してかつそれを置換することに係わる。その除去に続いて、そのＥＥＰＲＯＭを研究してその内容を解読する（ｄｅｃｈｉｐｅｒ）。次いで、解読した内容を使用して置換ＥＥＰＲＯＭをプログラムして、有効利用者勘定からＥＳＮ／ＭＩＮ対を着服する。このテクニックは、偽造者が一度に１つのＥＳＮを変えようと望むだけならば偽造者にとって魅力的であるかもしれない。しかし、この技術は、手数がかかり過ぎかつ未熟な偽造者は極めて慎重でない限りプリント配線を損傷するかもしれない。

偽造の精巧さにおける大きなステップは、電話マイクロプロセッサ・プログラム・コードを分析しかつそのコードの１つ以上の区分を書き換えて詐欺識別情報（ＥＳＮ／ＭＩＮ対）をセルラ基地局へ送信することに係わる。これは、しばしば、電話ハードウェア設計の逆エンジニアリングに係わり、埋め込まれたソフトウェア設計のかなりの理解を必要とする。しかしながら、この方法の明白な利点は、いったん改変が完了すると、電話を所望するだけ頻繁に新識別情報を用いてリプログラムできることである。

ほとんどの精巧な攻撃は、上に述べたセルラ電話のマイクロプロセッサ・コードの変更をハードウェア改変と組み合わせる。この技術の一例は、セルラ電話を最初に同調させるときのブートアップ・プロセス中にのみ実行する従来のメモリ

妥当検証ルーチンによる検出を回避するために、いわゆる「シャドウ・メモリ」を使用する。ブートアップ・プロセスは、コントローラ３００に含まれたブート・コード３０４の小部分に従って実行される（図３参照）。ブートアップ・プロセスは、セルラ電話をサービス条件に入れるように構成しかつマイクロプロセッサ３０１内のプログラム・カウンタをフラッシュ・メモリ３２０内の適当な位置へセットする。このプロセスが完了すると、コントローラ３００はＬＥＤ３１８（又は他の等価な信号）を点灯して利用者にその電話が使用中であることを表示する。偽造者は、下に更に詳細に説明するように、フラッシュ・メモリ３２０内の正規動作コードの実行を破壊するためにコントローラ３００とＬＥＤ３１８との間の接続３０６を監視することができる。

典型的最新セルラ電話に含まれたフラッシュ・メモリ３２０は、５１２Ｋのアドレス指定可能容量を有する。偽造者は、フラッシュ・メモリ３２０を除去し、かつ、元のフラッシュ・メモリの内容を１０２４Ｋシャドウ・メモリ３２２の初めの５１２Ｋ内へ複写した後、元のフラッシュ・メモリ３２０を１０２４Ｋシャドウ・メモリで置換することもできる。ブートアップ中、プログラム・メモリへのどのアクセスもフラッシュ・メモリ３２０の初めの５１２Ｋに成功裡に向けられる。次いで、偽造者は、将来の全てのプログラム・メモリ・アクセスをシャドウ・メモリ３２２へスイッチさせるために、ブート・プロセスが完了したことを表示する（ＬＥＤ信号３０６のような）電話内で利用可能な信号を監視することもできる。その後、セルラ電話は、シャドウ・メモリ３２２内にある命令に従って動作し、このメモリをタンブリング・ルーチン・コード及び相当するＭＩＮ／ＥＳＮ対を含むようにプログラムすることができる。

ほとんどのセルラ詐欺が或る程度のメモリ操作に基づいている理由から、連邦通信委員会（ＦＣＣ）は、セルラ電話詐欺のこの態様に対する解決を現在考え中である。この解決は、第２２．２１９章に示されたＦＣＣ規則案に組み込まれている。現在書かれているように、第２２．９１９章は、移動体電話の動作ソフトウェアが変更可能であることを禁止し、ＥＳＮが工場セットされて、いかなる方法でも変更、転送、除去又は操作されることが不可能であるように要求し、かつ移動体送信機が、もし製造業者を含むなんらかの者がセルラ電話のＥＳＮ、シス

テム論理、又はファームウェアを除去、いたずら、又は変化させようと企図するならば、動作不可能となることを要求する。

消費者の立場からは、現在の製造業者又はその工場が許可したサービス代理人の現在のセルラ電話をプログラムする能力は、適正に動作しないセルラ電話の置換を容易にしている。例えば、もし加入者のセルラ電話が適正に動作しないならば、その加入者は工場が許可した代理人から新装置を得かつそれを旧装置のものと同じ電子的な「個性（ｐｅｒｓｏｎａｌｉｔｙ）」を含むようにプログラムしてもらうことができる。セルラ電話の電子個性は、ＥＳＮだけでなく、利用者プロファイル及び個人及び／又は業務電話番号のような加入者によってその装置にプログラムされるかなりの量の情報もまた含む。修繕／置換プログラム及びセルラ電話にＥＳＮの変更及び他のメモリの変更を敏速かつ容易に加える技術は、欠陥端末によって自分達の加入者に不便をかけたくないセルラ・サービス提供業者達の主張で開発されてきた。

ＦＣＣ第２２．２１９章の下で、上に述べた状況にある加入者は、もしその旧移動体装置に欠陥があるならば、新装置を得ることが依然できることになる。しかしながら、新たな固定ＥＳＮが新装置と関連することになる理由から、新ＥＳＮ情報がセルラ通信事業者（ｃｅｌｌｕｌａｒ　ｃａｒｒｉｅｒ）へ通信されねばならず、通信事業者はそれを自分達のデータ・ベースにプログラムしなければならないことになる。この結果、長い時間中その加入者はサービスを受けられないことになる。加入者はまた、そのセルラ電話をなんらかの個人又は業務電話番号で以てプログラムしなければならないことになる。第２２．９１９章に関する遥かに顕著な問題は、セルラ・サービス提供業者が自分達の加入者のセルラ電話をプログラム又はリプログラムすることによってシステム・アップグレードを加入者に施すこれらサービス提供業者の能力に第２２．９１９章が与える逆影響である。

第２２．９１９章が、セルラ産業のシステムをアップグレードする能力へ実際に与える影響は、次のように言い表される。例えば、ＴＩＡ／ＥＩＡ／ＩＳ－１３６規格に指定されたようなディジタル制御チャネルの使用は、セルラ通信事業者に簡易文字メッセージ（ｓｈｏｒｔ　ｍｅｓｓａｇｉｎｇ）サービスのような

新しい拡張サービスを提供可能とする。もし通信事業者、製造業者、又は許可された代理店がセルラ電話のソフトウェア又はファームウェアに変化を加えることを許されるならば、このようなサービスを端末のソフトウェア・アップグレードを通じて加入者に敏速にかつ効率的に利用可能とすることができる。第２２．９１９章（その現在の形で）の下では、製造業者も、製造業者の許可したサービス代理人も、セルラ通信事業者も、このようなソフトウェア変化を加えることはできないことになる。通信事業者が加入者にシステム増強を提供することができる唯一の道は、加入者に新セルラ電話を購入するように要求することである。

加入者ばかりでなく製造業界への第２２．９１９章の影響を改善するために、ＦＣＣは、この規則が１９９５年１月１日後に初期型式承認（ｉｎｉｔｉａｌ　ｔｙｐｅ　ａｃｃｅｐｔａｎｃｅ）の申請が提出されたセルラ電話に適用されることになると声明した。事実、ＦＣＣは、１９９５年１月１日より前に提出された型式承認に対する申請に基づいて、現在動作中の２０００万のセルラ電話ばかりでなく１９９５年１月１日後にサービスに入った数１００万のセルラ電話をこの規則から適用免除してきている。電子情報を不法目的のために操作することができる非常に多くのセルラ装置が市場に出回っている事実は、第２２．９１９章が詐欺問題に極めて小さな影響しか与えないことを示唆している。ＥＳＮを用いて不法にいたずらすることによる詐欺に巻き込まれるこれらの対象物（ｅｎｔｉｔｙ）は、第２２．９１９章制約を受けない数１００万の端末を使用することによって引き続き詐欺に巻き込まれるおそれがある。

上述から承知できるように、安全メモリを有するセルラ電話を用意することが極めて望まれる。セルラ電話へのいたずらに対しこれらの電話を対抗性があるように改良する解決策は、現在、ないように思われる。更に、許可されたアクセスのみを保証するような方法で電子装置メモリに更新を施す方法及び装置はないように思われる。

## 概　要

セルラ電話メモリいたずら、及び全般的に電子装置メモリいたずらを防止する慣例の方法及び提案された解決のこれら及び他の欠点、及び限界が本発明によって克服され、本発明の模範的実施例が電子メモリ内容を無許可アクセス及び操作

から保護する。

本発明の一態様によれば、安全は、電子装置内の電子メモリ内容がいたずらされていないことを確かめるためにそれらの内容を周期的に監査することによって達成される。この監査は、このような内容の監査ハッシュ値、又は監査シグネチャを導出するために電子メモリの選択された内容にハッシュ計算を遂行することに係わる。監査ハッシュ値は、真正メモリ内容から先に導出された有効ハッシュ値と比較される。有効ハッシュ値は、好適には、暗号化された形で電子メモリ内へ記憶され、かつ比較目的にのみ復号される。監査ハッシュ値と有効ハッシュ値との間の不一致はメモリいたずらを表示することでき、したがって、その電子メモリを含む電子装置を動作不能させることができるか、又は警告表示を行うことができる。

本発明の他の態様によれば、（セルラ電話のＥＳＮを含む）セルラ電話メモリに含まれた内容のような電子メモリ内容を、そのメモリ内容にアクセスを許される前に、認証されているデータ転送装置によって更新することができる。データ転送装置認証は、公衆／私用キー認証方式の使用に係わる。データ転送装置が電子装置とインタフェースしかつアクセスをリクエストするとき、電子装置はデータ転送装置を認証するプロセスを開始する。これは、一連のメッセージを電子装置とデータ転送装置との間で交換することに係わることができる。公衆キーは、暗号化されたメッセージを復号するために使用される電子装置内に維持されるか、又はデータ転送装置内に維持された安全私用キーで以て「符号付け（ｓｉｇｎｅｄ）」される。特に、データ転送装置が電子装置をプログラムするようにリクエストするとき、認証プロセスが開始される。電子装置は、データ転送装置へ呼び掛けメッセージを送ることによって応答する。呼び掛けメッセージは、データ転送装置内に維持された私用キーを使用してディジタル・シグネチャで符号付けされる。符号付き呼び掛けメッセージは電子装置へ送り返され、電子装置はこのメセージを公衆キーを使用して認証する。いったん認証されると、データ転送装置は、電子装置内の特権命令及び能力にアクセスすることを許される。

電子メモリの何らかのリプログラミングに続いて、電子装置は新（有効）ハッシュ値を導出するハッシュ計算を改変されたメモリ内容において遂行する。新ハ

ッシュ値が、私用キーによるディジタル・シグネチャのためにデータ転送装置へ返される。符号付き新ハッシュ値が記憶されるためにデータ転送装置へ返される。電子装置が後続メモリ監査を遂行するとき、結果のハッシュ値が新有効ハッシュ値と比較される。

## 図面の簡単な説明

本発明の上述の及び他の目的、特徴及び利点が、添付図面と関連したこの説明を読むとき更に容易に理解される。これらの図面で、

図１はセルラ通信システムの理想的レイアウトを示す線図である。

図２はセルラ呼を設定する慣例のセルラ認証方法を示す流れ図である。

図３は慣例のセルラ電話プロセッサ及びメモリ構成を示すブロック図である。

図４は本発明の模範的実施例に従うセルラ電話プロセッサ及びメモリ構成を示すブロック図である。

図５は本発明の実施例に従う模範的セルラ電話立ち上げプロセスを示す流れ図である。

図６は本発明に従う模範的周期的メモリ妥当検証プロセスを示す流れ図である。

図７は本発明の実施例に従う模範的データ転送装置を示すブロック図である。

図８は本発明の実施例に従ってデータ転送装置を認証する模範的プロセスを示す流れ図である。

図９は本発明の実施例に従って初期ＥＳＮをセルラ・メモリ内へ入力する模範的プロセスを示す流れ図である。

図１０は本発明に従って確立されたＥＳＮをリプログラムする模範的プロセスを示す流れ図である。

図１１は本発明の模範的実施例に従って保護されたメモリ構成を示すブロック図である。

図１２は本発明の実施例に従う模範的セルラ電話プログラマを示すブロック図である。

## 詳細な説明

本発明に従う装置及び方法に係わる模範的電子メモリが、セルラ電話応用につ

いての文脈の中で下に開示される。下に説明される例は、単に、本発明を組み込む理想的応用を解説するために与えられる。

図４で、コントローラ４００がセルラ電話（例えば、図１２の参照符号１２０４を参照）を制御する。コントローラ４００は、フラッシュ・プログラム・メモリ４２０、電子的消去可能プログラマブル読み出し専用メモリ（ＥＥＰＲＯＭ）４１０、及びランダム・アクセス・メモリ（ＲＡＭ）４０８と連携して動作する。コントローラ４００は、マイクロプロセッサ４０２及び内部読み出し専用メモリ（ＩＲＯＭ）４０３を含む。ＩＲＯＭ４０３は、ブート・コード４０４、ハッシュ・コード４０５、認証コード４０９、及び公衆暗号化キー４０６を含む。コントローラ４００はまた、保護スタティック・ランダム・アクセス・メモリ（ＰＳＲＡＭ）４０７、割り込みコントローラ４２１、及び選択されたメモリ内容へのマイクロプロセッサ４０２による周期的ハッシュ計算を開始させるめのハードウェアに基づくタイマ４０１を含む。ＥＥＰＲＯＭ４１０は、利用者プロファイル・データ４１２、ＥＳＮ４１４、ＭＩＮ４１６、及び符号付き／符号なし有効ハッシュ値対４１８を含む。セルラ電話の全般動作に係わる命令コードがフラッシュ・プログラム・メモリ４２０に含まれる。ＲＡＭメモリ４０８は、正規セルラ電話呼処理の部分である動作のためのスクラッチパッドとして使用される。感応性データ、ハッシュ値計算及び認証プロセスに係わる動作は、好適には、ＰＳＲＡＭ４０７と連携して実施される。コントローラ４００は、メモリ・バス４２４を経由して、フラシュ・プログラム・メモリ４２０、ＲＡＭ４０８、及びＥＥＰＲＯＭ４１０と通信する。

本発明の模範的実施例による、図４に示されたシステムに対する電話電源投入及びメモリ妥当検証のプロセスを図５に示す。セルラ電話がターン・オンされた後、コントローラを初期化するために、ＩＲＯＭ４０３内のブート・コード４０４がマイクロプロセッサ４０２によって実行される（ブロック５００）。フラッシュ・プログラム・メモリ４２０の選択された内容及びＥＥＰＲＯＭ４１０に記憶されたＥＳＮ値４１４に監査ハッシュ値計算を遂行するめに、ＩＲＯＭ４０３内に含まれたハッシュ・コード４０５がランされる（ブロック５０２）。次いで

、コントローラは、ＥＥＰＲＯＭ４１０に記憶された符号付きハッシュ値対４１８を認証する（ブロック５０４）。これは、符号付き有効ハッシュ値を公衆キー４

０６で以て処理し、次いでその結果を符号なしハッシュ値と比較することによって符号付き有効ハッシュ値を認証することを伴うことがある。認証されたハッシュ値が、次いで、ＰＳＲＡＭ４０７に記憶される（ブロック５０６）。ブロック５０２で導出された監査ハッシュ値が、次いで、ブロック５０４で導出された認証されたハッシュ値と比較される（ブロック５０８）。もしこれら２つのハッシュ値が一致するならば、マイクロプロセッサ・プログラム・カウンタがフラッシュ・メモリ４２０内の適当な位置にセットされ、かつ周期的ハッシュ計算プロセスが使用可能とされ（ブロック５１０）、その後、セルラ電話は正規動作を開始する（ブロック５１２）。もしハッシュ値がブロック５０８で一致しないならば、このシステムは無限ループに置かれ（ブロック５１４）、そうでなければ、使用禁止される。上述のプロセスは偽造者が改変したプログラムをフラシュ・メモリに代入する又は改変したＥＳＮをＥＥＰＲＯＭ４１０へ代入するのをどちらも防止する。これは、そのようにしようとするとハッシュ値の不一致を起こし、それによって電話を動作不能にすることになるからである。

正規動作の開始に続いてシャドウ・メモリ４２２を有効フラッシュ・メモリ４２０に代入するのを防止するために、周期的ハッシュ値処理を遂行するのが好適である。正規電話動作中、周期的ハッシュ値計算がタイマの期限切れ又はその他のシステム事象に応答して行われる。図４に示された模範的実施例では、周期的ハッシュ計算は、ハードウェア・ベース・タイマ４０１の期限切れに応答して開始され、このタイマはマスク不可能割り込み（ｎｏｎ－ｍａｓｋａｂｌｅ　ｉｎｔｅｒｒｕｐｔ；ＮＭＩ）を発生させる。ＮＭＩは、ソフトウェア・プロセスによって「マスク」出力することができないハードウェア向きプロセスでる。したがって、偽造者は、ＮＭＩを無視するように設計されるシャドウ・コードを構成することができない。正規（ｒｅｇｕｌａｒ）割り込みもまたハードウェア割り込みであって、これはマイクロプロセッサ資源にアクセスを取るために正規セル

ラ電話事象からの他の正規割り込みと競争しなければならない。正規割り込みは、それがサービスをリクエストする最高優先権割り込みになるとき、肯定応答されかつ処理される。

完全なハッシュ値計算は正規（ｎｏｒｍａｌ）電話動作によって容認され得る

よりも長くかかることがあるから、時間間隔（例えば、数秒）にわたって分散したいくつかのセグメントで断片式に処理を遂行するのが好適である。本発明の他の態様に従って、ハードウェア・ベース・タイマは、ハッシュ値計算のセグメントを遂行するために２つのステップを呼び起こす。第一に、マスク不可能割り込み（ＮＭＩ）がマイクロプロセッサに周期的ハッシュ計算に含まれる予定の次のフラッシュ・メモリ又はＥＥＰＲＯＭメモリ位置の内容を直ちに検索させ、かつそれをＰＳＲＡＭに記憶させる。ＮＭＩは、短い、最高優先権の割り込みの種類のものであって、これはＮＭＩが起こるとき活性であることがあるマイクロプフロセッサ・タスクにほとんど無視できる影響しか与えない。これは、ハッシュ計算による検出を免れるように偽造ソフトウェアが行動を起こし得ないことを保証する。第二に、低優先権標準割り込みがハードウェア・ベース・タイマ４１０によってまた発生され、この割り込みはＮＭＩルーチンによって先に捕獲されたメモリ・バイトに基づいてハッシュ値計算の現在セグメントを完了するサービスをリクエストする。このタスクは、ハードウェア・タイマが期限切れしかつ電話を使用禁止する前に、正規呼処理タスクのために必要とされるに従って、所定最長時間（Ｔ）だけ延期されてよい。最長時間（Ｔ）は、どれかの正当呼処理を完了するために、ハッシュ計算セグメントを仕上げるために、及びハードウェア・タイマをそれが期限切れになる前にそのカウントダウン・サイクルの開始にリセットするために、適当であるように選択される。ハッシュ値計算のセグメントを周期的に完了するために２つの型式の割り込みを使用する戦略は、システム応答のいかなる劣化も回避する一方、安全検査がシャドウ・メモリ内に在駐する偽造ソフトウェアによって迂回され得ないことを保証する。

本発明に従う模範的周期的ハッシュ値計算を示す流れ図を図６に示す。この図を参照すると、ハードウェア・タイマ４０１内のＴ１カウンタが期限切れすると

（ブロック６０２）、ブロック６０４でＮＭＩ及び正規割り込みの両方が起こる。いったんＮＭＩがマイクロプロセッサの制御を得ると（ブロック６０４）、このシステムは短い時間間隔中、正規割り込みを使用禁止するか又は待ち行列させ、この時間間隔中、ハッシュ計算に必要とされるフラッシュ・メモリ内又はＥＥＰＲＯＭメモリ内の次のバイトがＰＳＲＡＭ内へ複写される（ブロック６０６）。

次いで、制御は、ＮＭＩが起こったとき実行するタスクへ復帰する（ブロック６０８）。正規条件の下で、短い時間間隔内に、ハードウェアに基づくタイマ４０１からの正規割り込みも供給され（ブロック６１０）、かつハッシュ計算のセグメントがＰＳＲＡＭに先に記憶されたメモリ・バイトに基づいて完了される（ブロック６１６）。もしハッシュ値計算が未だ完了しないならば、ハードウェア・ベース・タイマ（Ｔ１及びＴ２）４０１がそれらの初期値にリセットされ（ブロック６２４）、かつタイマＴ１の次の期限切れまで正規電話動作が続く（ブロック６００）。正規割り込みが供給される（ブロック６１０）前にもし万一タイマＴ２が期限切れする（ブロック６１２）ならば、電話は使用禁止される（ブロック６１４）。（正規割り込みが正しく供給されない限り）タイマＴ２のデフォールト期限切れは、偽造者が周期的ハッシュ計算を使用禁止とするのを防止する。

監査ハッシュ値計算が完了する（ブロック６１８）まで、ハッシュ値のこの周期的断片状計算は続く。先に認証されたハッシュ値が、次いで、ＰＳＲＡＭから取り出されてかつ監査ハッシュ値と比較される（ブロック６２０）。もし一致すれば、ハードウェア・ベース・タイマ４０１がリセットされ（ブロック６２４）かつ電話は正規に動作し続ける（ブロック６００）。もし不一致であるならば、このシステムは、例えば、マイクロプロセッサ４０２を停止条件に置くことによって使用禁止される（ブロック６２２）。

ハッシュ計算を好適には遂行されるセルラ電話メモリの選択された内容は、フラッシュ・メモリ４２０からの内容及びＥＥＰＲＯＭ４１４内のＥＳＮを含む。これは、偽造者がフラッシュ・メモリ又はＥＥＰＲＯＭのどちらかを物理的に除去しかつそれらをセルラ通信事業者を詐欺するように設計された改変ＥＳＮ及び

／又はプログラム・コードを含むリプログラムされた装置で以て置換するのを防止する。選択されたメモリ内容及び使用されたハッシュ値が、そのハッシュ値計算に含まれたメモリのたとえ１ビットの改変によっても電話を動作不能にさせることが好適である。

本発明の他の態様に従って、セルラ電話をデータ転送装置を使用して安全な方法でプログラムすることができる。本発明に従う模範的データ転送装置を図７に示す。コントローラ４００の参照番号、その内容、及び関係したメモリは、図４

のものと同じである。模範的データ転送装置７５０が安全マイクロプロセッサ７５２を含み、このマイクロプロセッサは私用暗号化キー７５４を含み、このキーはコントローラ４００内のＩＰＲＯＭ４０３内の公衆暗号化キー４０６に相当する。安全マイクロプロセッサ７５２は、インタフェース７５８を経由してセルラ電話コントローラ４００と通信する。インタフェース７５８は、ＲＳ－２３２リンクのような有線直列接続、無線赤外線インタフェース、又はセルラ電話の主アンテナ（図示してない）又はセルラ電話内の他のアンテナのようなＲＦインタフェースであってよい。

データ転送装置７５０によるセルラ電話メモリへのアクセスは、厳格な認証プロセスが完了した後に限り許される。更に明細に述べるならば、コントローラ４００（及び関係したメモリ構成要素）は、データ転送装置７５０がその真正を保証するために呼び掛け応答プロセスを受けた後に限りデータをダウンロードする目的のためにアクセスすることができる。図８は、本発明の模範的実施例に従ってデータ転送装置７５０を認証する模範的プロセスを示す。第１ステップ（ブロック８００）として、電話は、好適には、図５に関して先に説明した詐欺防止プロセスを使用して、動作条件にもたられる。インタフェースが確立された後、安全プロセッサ７５２がプログラミング・リクエスト・メッセージを、安全マイクロプロセッサ７５２によって発生された乱数（Ｒａｎｄ１）と一緒に、コントローラ４００へ送る（ブロック８０２）。応答して、コントローラ４００は、乱数呼び掛けコード（Ｒａｎｄ２）を安全マイクロプロセッサ７５２へ送る（ブロック８０４）。次いで、安全マイクロプロセッサ７５２は、Ｒａｎｄ１、Ｒａｎｄ

２及び私用キー７５４に基づいて呼び掛け応答を発生する（ブロック８０６）。次いで、呼び掛け応答がコントローラ４００へ返される（ブロック８０８）。呼び掛け応答は、Ｒａｎｄ１、Ｒａｎｄ２、及び公衆キー４０６を使用してコントローラ４００によって処理される（ブロック８１０）。処理された呼び掛け応答は、次いで、その値をＲａｎｄ２と比較されることによって認証される（ブロック８１２）。もし呼び掛け応答が（例えば、Ｒａｎｄ２）が適正に復号するならば、データ転送装置の認証が妥当検証されかつ電話はプログラミング・モードへ入る（ブロック８１４）。その後、データ転送装置７５０は、セルラ電話内の種

種のメモリにアクセスする及び／又は新フラッシュ・メモリ４２０内容をダウンロードすることができる。

もし呼び掛け応答が有効でないならば、故障カウントが増分される（ブロック８１６）。故障カウントは、それが所定数（最大カウント）に到達したかどうかを見るために検査される（ブロック８１８）。故障カウントは、データ転送装置７５０が雑音性媒体を通じてコントローラ４００と通信中であるかもしれないことを考慮に入れる。どんな結果の送信誤りも認証故障を生じると云ってよい。それゆえ、セルラ電話をプログランミング・モードに置く２回以上の機会をデータ転送装置７５０に与えるのが好適である。本発明の模範的実施例では、５０の最大カウントが適当であると判定された。もし最大数に達しなかったならば、認証故障が起こったことを表示するメッセージがデータ転送装置７５０へ送られる（ブロック８２２）。このような表示を受信すると、認証プロセスがブロック８０２で再開始する。もし所定数の企図に達したならば、電話は動作不能条件に置かれかつ電話が許可されたサービスへ復帰しなくてはならないことを利用者に示すメッセージを表示することができる。

データ転送装置７５０がなんらかのＥＳＮリプログラミング又はフラッシュ・メモリ４２０へダウンロードすることを完了した後、電話内のコントローラ４００は新ハッシュ計算を開始し、この計算は、例えば、フラッシュ・メモリ４２０の改訂内容及びＥＳＮ４１４を含む。結果のハッシュ値が、私用キー７５４を使用するディジタル・シグネチャのためにデータ転送装置７５０へ送られる。次い

で、符号付きハッシュ値が、同じハッシュ値の符号なしのものと一緒に、ＥＥＰＲＯＭ４１０に記憶されるめにコントローラ４００へ返される。

ＥＳＮを本発明に従ってリプログラムすることができるが、しかし安全理由から、ＥＳＮプログラミングは、好適には、認可された工場代理人ではなく、工場レベルで行われる。ＥＳＮのプログラミングは、２つの状況で起こる得る。すなわち、製造中の初期ＥＳＮプログラミング、及び現存するＥＳＮのリプログラミング。初期ＥＳＮは、図７のそれに類似のデータ転送装置を使用してプログラムすることができる。初期ＥＳＮプログラミング・プロセスを図９に関して下に説明する。

第１ステップ（ブロック９００）として、電話を動作状態にする（図５参照）。この電話とのインタフェースの確立に続いて、安全プロセッサ７５２がＥＳＮプログラミング・リクエスト・メッセージを、乱数（Ｒａｎｄ１）と一緒に、コントローラ４００へ送る（ブロック９０２）。コントローラ４００は、新たに製造された電話の場合の常として電話内のＥＳＮが全てゼロであるかどうか判定する検査を遂行する（ブロック９０６）。もしＥＳＮが全てゼロでないならば、ＥＳＮプログラミング・モード・リクエストは否定される（ブロック９０６）。もしＥＳＮが全てゼロであるならば、図８のステップ８０４から８２０で設定されたのと実質的に類似した呼び掛け応答プロセスが開始される（ブロック９０８）。データ転送装置７５０の成功認証に続いて、新ＥＳＮをＥＥＰＲＯＭ４１０内へダウンロードすることができる。

データ転送装置７５０がＥＳＮをＥＥＰＲＯＭ４１０内へダウンロードするのを完了した後、コントローラ４００は、新ＥＳＮ４１４を含む新ハッシュ計算を開始する。結果のハッシュ値が、私用キー７５４を使用するディジタル・シグネチャのためにデータ転送装置７５０へ送られる。次いで、符号付きハッシュ値４１８が、ＥＥＰＲＯＭ４１０に記憶されるために、同じハッシュ値の符号なしのものと一緒に、コントローラ４００へ返される。

現存するＥＳＮをまた、本発明を組み込むシステム内でリプログラムすることができる。ＥＳＮリプログラミングは、好適には、工場でのみ行われ、地方の許

可された工場代理人によっては行われない。電話内へ先にプログラムされたＥＳＮを変える目的のためにこの電話内へロードされてある、工場でのみ利用可能な１組のマイクロプロセッサ命令を利用することによって、安全が追加される。このプロセスは図７に示したものと類似のデータ転送装置を使用して実施することができ、これを図１０に関して以下に説明する。

第１ステップ（１０００）として、電話を、図８に示したプロセスに従って正規プログラミング・モードにする。工場データ転送装置７５０はＥＳＮリプログラミング・コード７５６を含み、このコードは、ＥＳＮリプログラミングを容易にするために、セルラ電話のＰＳＲＡＭ４０７内へダウンロードすることができる。システムをプログラミング・モードにしたなら、ＥＳＮリプログラミング・

コード７５６がＰＳＲＡＭ４０７内へダウンロードされる（ブロック１００２）。ＥＳＮリプログラミング・コード７５６を実行するに当たって、コントローラ４００は、現存するＥＳＮをゼロにし（ブロック１００４）、かつＥＳＮリプログラミング・プロセスを開始する（ブロック１００６）。

データ転送装置７５０が新ＥＳＮをＥＥＰＲＯＭ４１０に入力するのを完了した後、コントローラ４００は新ハッシュ計算を開始し、この計算は新ＥＳＮ４１４を含む（ブロック１００８）。結果のハッシュ値が、私用キー７５４を使用するディジタル・シグネチャのためにデータ転送装置７５０へ送られる（ブロック１０１０）。次いで、符号付きハッシュ値４１８が、ＥＥＰＲＯＭ４１０に記憶されるために、同じハッシュ値の符号なしのものと一緒に、コントローラ４００へ返される（ブロック１０１２）。

本発明の模範的実施例でのハッシュ値計算及びディジタル・シグネチャは、片方向ハッシュ化関数及び私用／公衆キー認証方式を使用して実施される。片方向ハッシュ関数は、セルラ電話内のメモリ内容を表すハッシュ値を導出するために使用される。公衆／私用キー方式は、ＥＥＰＲＯＭに記憶された有効ハッシュ値の安全を確保しかつセルラ電話内のメモリを操作しようと企図するデータ転送装置又はプログラマを認証するために使用される。片方向ハッシュ化は、当業者に知られており、かつ、例えば、ムーア（Ｍｏｏｒｅ）の米国特許第５，３４３，

５２７号に説明されている。

片方向ハッシュ関数は、順方向に計算するのが容易であるが、逆方向に計算するのが困難な関数である。片方向ハッシュ関数Ｈ（Ｍ）は任意長入力Ｍに演算し、この入力は、本発明の模範的実施例では、選択された電子メモリ内容で構成される。Ｍに遂行されたハッシュ関数は、固定長ハッシュ値ｈを生じる（式１参照）。

$$h = H(M) \qquad \text{式1}$$

任意長入力を取りかつ固定長の出力を生じることができる多くの関数があるが、しかし片方向ハッシュ関数は次の追加特徴を有する。すなわち、Ｍが与えられると、ｈを計算するのが容易である。ｈが与えられても、Ｍを計算するのが困難で

ある。及び、Ｍが与えられると、Ｈ（Ｍ）＝Ｈ（Ｍ’）のような他のメッセージＭ’を見付けるのが困難である。

片方向ハッシュに対する基本的な攻撃は、次のようである。すなわち、メモリ内容（ハッシュ化内容）のハッシュ値が与えられると、偽造者は、Ｈ（Ｍ）＝Ｈ（Ｍ’）のような、メモリ内容Ｍ’の他の組を作成しようと努めるであろう。もし偽造者がこれを行うのに成功したとしたならば、この片方向ハッシュ関数の安全をひそかに崩すであろう。片方向ハッシュ関数の目的は、Ｍに固有のシグネチャ、つまり、指紋を用意することである。本発明では、安全片方向ハッシュ関数は、監査ハッシュ値を用意するためにセルラ電話メモリの選択された内容について遂行される。監査ハッシュ値は、メモリからの真正であると知られている選択されたメモリ内容に基づいて片方向ハッシュ関数を遂行することによって、先に発生された有効ハッシュ値と比較される。

好適実施例では、ＭＤ５のようなメッセージ・ダイジェスト・アルゴリズムが、安全片方向ハッシュ計算に使用される。ＭＤ５アルゴリズムは、入力メッセージのＮビット・ハッシュ、つまり、メッセージ・ダイジェスト（すなわち、選択されたメモリ内容）を発生する。ＭＤ５アルゴリズムは、選択された内容中の単

一ビットに変化を生じると統計的にそのハッシュ値ビットの半分に変化を生じさせるという点で、非常に敏感である。ＭＤ５アルゴリズムはまた、その速度及び簡単性のために知られている。速度は、セルラ電話のマイクロプロセッサに課せられた時間要求が通常のシステム・プロセスと許容不能に干渉するほどに大きいものであってはならないという点で、重要な考慮すべき問題である。

ＭＤ５アルゴリズムはまた、このアルゴリズムを増分式に遂行することができ、それによってハッシュ・プロセスの割り込みを許し、その結果、ハッシュ化を再び始める前に通常のマイクロプロセッサのタスクに取り組むことができるという理由で適している。更に、ＭＤ５アルゴリズムは、従来のマイクロプロセッサ・アーキテクチャに使用されるのにも充分適している。本発明の実施例に従って使用することができる他の片方向ハッシュ・アルゴリズムには、次のものがあるが、これらに限られるわけではない。すなわち、Ｓｎｅｒｆｕ、Ｈ－Ｈａｓｈ、ＭＤ２、ＭＤ４、Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ（ＳＨＡ）、及びＨ

ＡＶＡＬ。当業者ならば、片方向ハッシュ・プロセスを実行するようにマイクロプロセッサを容易にプログラムすることができる。

公衆キー・アルゴリズムは２つのキーを使用し、１つは公に利用可能であり、１つは私的に（秘密を）保つものでメッセージ暗号化及び復号、メッセージ認証、及びディジタル・シグネチャのようなタスク用である。これらのキーは、異なる目標を達成するために異なる方法で使用することができる。例えば、もし目的がメッセージを秘密に維持することであるならば、受信者だけがメッセージを復号できるように受信者が私用キーを安全に維持するべきである。このような場合、暗号化キーは、公に知られかつ特定の潜在受信者と関連していることが知られ得る。送信者はこのプロセスで情報の安全を保証される得るけれども、受信者は送信者の真正を保証され得ない。もし一対のキーのうちの私用（秘密）キーが送信者によって暗号化用に秘密に維持されるならば、対応する公衆キーを持つどの受信者も、安全の保証はないものの、送信者の真正を保証され得る。本発明に従ってデータ転送装置を認証することに利用されるのは、後者の方式である。

公衆キー・アルゴリズムは数学的トラップドア関数に基づいて演算し、この関数は公衆キーから私用キーを演算することを計算上実行不可能にする。周知のＲＳＡ（Ｒｉｖｅｓｔ、Ｓｈａｍｉｒ、ａｎｄ　Ａｄｌｅｍｅｎ（リヴェスト、シャミア、エイドルマン））アルゴリズムの場合、２つの大きな素数の積を因数分解するのが困難であることに基づいている。キー選択は、２つの大きな素数ｐ及びｑの選択で始まり、これらは互いに乗じられて、大きな数ｎを生じる。

$$n = pq \qquad \text{式２}$$

次いで、暗号化キーｅは、ｅと(p-1)(q-1)とが相対的に素数であるようにランダムに選択される。最後にユークリッドのアルゴリズムを使用して、復号キーｄが次のように計算される。

$$F = (p-1)(q-1) \qquad \text{式３}$$

$$ed = 1 (\text{mod } F) \qquad \text{式４}$$

数ｅ及びｎは公衆キーであり、数ｄは私用キーである。式５がＲＳＡ暗号化プロセスを与え、及び式６が復号化プロセスを与える。

$$C = M^e (\text{mod } n) \qquad \text{式５}$$

$$M = C^d (\text{mod } n) \qquad \text{式６}$$

因数ｎを求める能力のある敵は、式３を使用して係数Ｆを決定し、次いで、公衆キーｅが与えられるならば、式４から私用キーｄを決定することができるかもしれない。それにもかかわらず、上に注意したように、ｎは、普通、非常に大きいからこのような因数分解を実行不可能にする。ＲＳＡアルゴリズムについての更に詳細は、リヴェスト他の米国特許第４，４０５，８２９号に見ることができる。

本発明の好適実施例では、フィアット・シャミア（Ｆｉａｔ－Ｓｈａｍｉｒ；ＦＳ）アルゴリズム又はその傍系が利用される（米国特許第４，７４８，６６８号が参考になり、この特許の内容は言及することによってその内容が本明細書に全面的に組み込まれている）。ＦＳアルゴリズムは認証及びディジタル・シグネチャ方式を実現するために適しており、この方式は典型的セルラ電話の限定され

た計算能力に充分適している。

ＦＳアルゴリズムは、このアルゴリズムがｎを法とする平方余剰($v_i$)の逆数を見付けることが困難であることに基づいて因数を使用すると云う点で、ＲＳＡのような、先の方式と異なっている。更に明細に述べると、ＦＳ方式は、好適には、長さで５１２ビットから１０６４ビットまでの２つの大きな素数の積である数ｎを選択することに係わる。公衆キー(v)：$v_1, v_2, \cdots v_k$,及び私用キー(s)：$s_1, s_2, \cdots s_k$,は$s_i = sqrt(1/-v_i) \bmod n$のように発生される。上掲の式についての文脈の中で逆数$(1/-v_i) \bmod n$を見付ける困難が素数ｎの因数を見付ける困難と等価であることを示すことができる。安全性を犠牲することなく、このアルゴリズムは他の方式よりも遥かに敏速に実行する。事実、ＦＳ方式は、必要な認証計算を完了するた

めに通常要するモジュラ乗算の１％から４％をＦＳ計算が必要とするに過ぎないと云う点でＲＳＡ方式よりも性能的に優れていることが判っている。これは、同じタスクを遂行するためにＲＳＡ方式を使用するよりも２桁まで高い速度で符号付きハッシュ値を認証することに相当する。したがって、データ転送装置認証及び周期的監査ハッシュ値比較をＲＳＡ方式よりもＦＳ方式を使用してかなり速く遂行することができる。工場レベルでセルラ電話メモリ又はその他の電子メモリを大量にプログラムするとき、ＦＳアルゴリズムの使用は記憶する有効ハッシュ値のディジタル・シグネチャをより敏速に発生することによって生産時間を短縮する。応用することができるアルゴリズムには、次に限られるわけではないが、ＥＬＧＡＭＡＬ、ＤＳＡ、及びフィージ・フィアット・シャミア（Ｆｉｅｇｅ－Ｆｉａｔ－Ｓｈａｍｉｒ）がある。

本発明の他の態様によれば、セルラ電話内のコントローラ・ハードウェアは、偽造者が安全メモリの内容を判定すること、あるいは先に説明した安全方式を迂回することを防止する安全特徴を有する。図１１は、コントローラ・ハードウェア、外部メモリ、及びメモリ／アドレス・バス構造の細部を示す。チップ選択論理１１２２及び安全論理１１２４を除いて、コントローラ内の構成要素の機能及び動作は、図４について説明したのと同じである。チップ選択論理１１２２は、

マイクロプロセッサ・アドレス・バス１１０２に接続されたメモリ構成要素及びハードウェア装置に対してハードウェア選択信号を供給するためにバス１１０２上のアドレスをデコードする。例えば、ＩＲＯＭメモリ４０３に割り当てられるアドレスがアドレス・バス１１０２上に現れる時はいつでも、ＩＲＯＭチップ選択（ＣＳ）が使用可能にされる。

安全論理１１２４は、ＩＲＯＭメモリ４０３以外のメモリ装置に記憶されたマイクロプロセッサ命令コードを使用してＰＳＲＡＭ４０７の内容にアクセスする又はハードウェア・ベース・タイマ４０１をリセットする企図を検出するように機能する。例えば、ＰＳＲＡＭ４０７内のメモリ位置の目標アドレスを用いてのフラッシュ・メモリ４０２に置かれた読み出し又は書き込み命令は、違法動作として検出されることになる。どんな違法アクセス企図もマイクロプロセッサを停止状態に入らせ、停止状態はセルラ電話が正規動作を回復するために電話の完全な電源リセットを必要とする。

安全論理は、次の論理式を実現することである。すなわち、

論理式１　　$S = \uparrow Supvr \bullet B$

論理式２　　$Halt = \text{not } S \bullet (A + C)$

ここに、
- Ｓ　＝　安全モード、
- ↑Ｓｐｕｒｖ＝　マイクロプロセッサの監視モードへの遷移、
- Ａ　＝　ＰＳＲＡＭメモリに対するチップ選択信号、
- Ｂ　＝　ＩＲＯＭメモリに対するチップ選択信号、
- Ｃ　＝　ハードウェア・タイマに対するチップ選択信号、
- Ｈａｌｔ＝　マイクロプロセッサへのハードウェア制御入力であって、マイクロプロセッサを無際限ループに入れる、又は電源が除かれかつ電話に再印加されるまで待機させる。

上の論理式１は次のことを述べる。すなわち、マイクロプロセッサが監視モード

へ遷移し（↑Ｓｕｐｅｒｖ）、それと同時にＩＲＯＭ４０３が活性である（・Ｂ）とき常に安全モード（Ｓ）がセットされる。論理式２は次のことを述べる。すなわち、もしコントローラ４００が安全モードになく（ｎｏｔＳ）かつＰＳＲＡＭ４０７選択又はハードウェア・タイマ・チップ選択のどちらかが活性である（・（Ａ＋Ｃ））ならば、マイクロプロセッサ停止入力が活性化される。この論理は、ＰＳＲＡＭ４０７への適法アクセス及びハードウェア・タイマ４０１へのリセット命令が、好適には、ＩＲＯＭ４０３に記憶されたコードに由来するから、先に説明したハッシュ値比較及び認証プロセスによって提供される安全処置の迂回を有効に防止する。

ＩＲＯＭメモリ４０３に置かれた全ての適法コード（ブート・コード、アッシュ・コード、公衆キー・コード、及び認証コード）が、好適には、命令によって括弧に入れられ、これが安全モードをルーチンの開始にセットさせ及びそのルーチンを去るときクリアさせる。本発明の好適実施例では、ソフトウェア割り込み命令（最近のマイクロプロセッサでは普通利用可能である）がＩＲＯＭ４０３内各ルーチンの開始に置かれて、マイクロプロセッサ４０２を監視モードへスイッチしかつマイクロプロセッサ・ハードウェア信号ＳＰＶＲを活性になるようにさせる。ＩＲＯＭ４０３チップ選択信号はそのとき活性であるから、安全モードＳがセットされる。そのソフトウェア・ルーチンの終わりで復帰命令を実行して、安全モードを取り消す。

本発明の他の態様によれば、データ転送装置は工場供給安全装置を含み、この装置は汎用コンピュータとの組み合わせで使用することができる。安全装置１２００は、標準コネクタ１２０６を経由してＰＣ１２０２の入力出力ポートに取り付けられる。ＰＣ１２０２上の第２ポートは、ＲＳ－２３２、ケーブル、又は赤外線リンクのような第２標準コネクタ１２０８と連携して使用され、セルラ電話１２０４とインタフェースする。図８に示したプロセスは、セルラ電話リプログラミング・プロセスを実施するために図１２に示した構成を使用して遂行することができる。標準ＰＣ及び安全装置１２００を有する許可された工場サービス代理人は、電話をリプログラムする装備を有する。

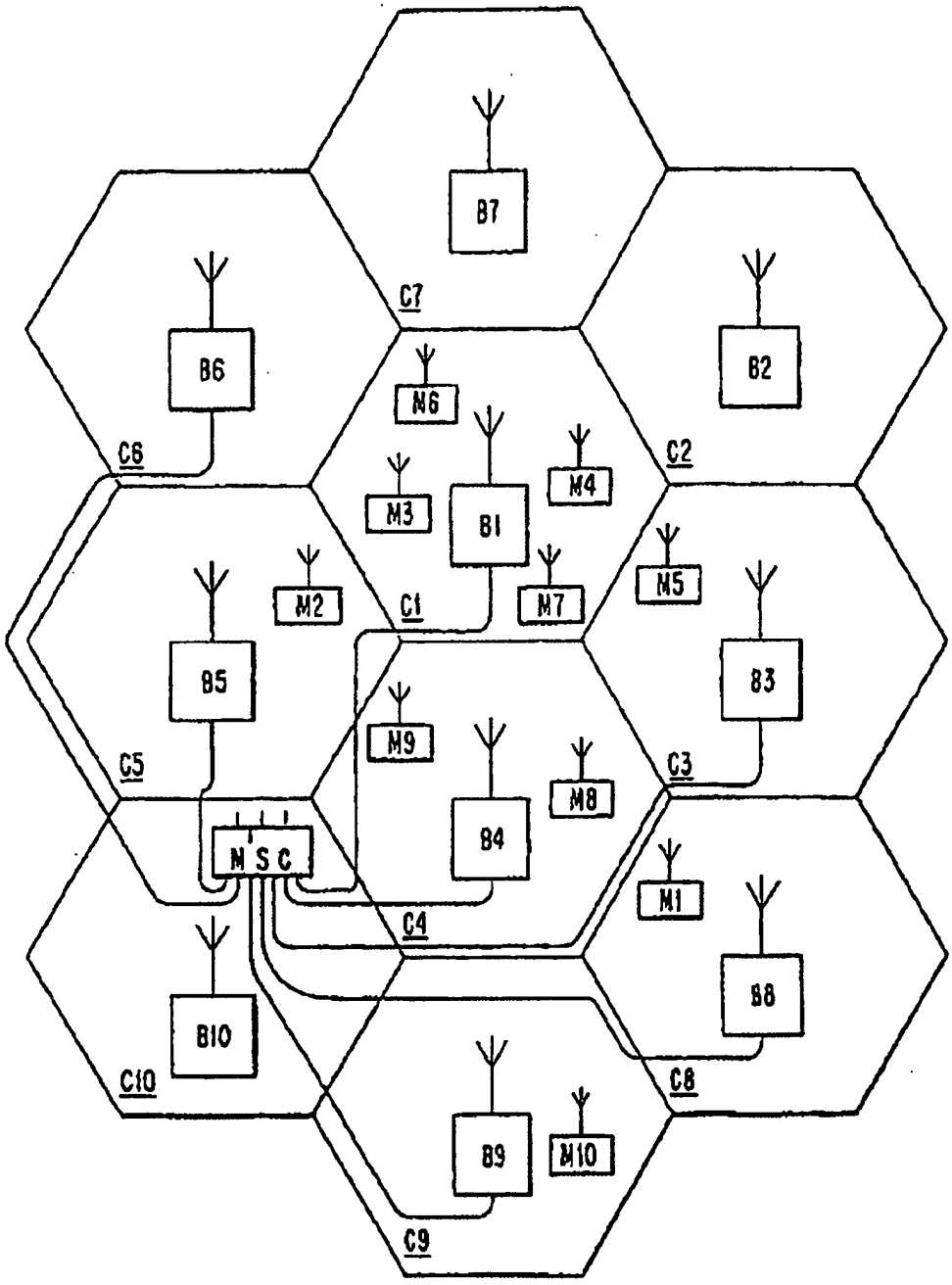
本発明の他の実施例によれば、現存するセルラ電話は、内部プリント配線板カードアッセンブリにアクセスすることによらない攻撃に対して安全であるフィールド・プログラミング能力を備えることができる。この保護レベルは、外部電話コネクタを通してアクセス可能な試験命令を使用して電話内のメモリ内容を改変する偽造攻撃の最も普通の方法に対して非常に効果的である。これは、フィールド・プログラミング命令にアクセスを容認するのに先立ち、図８で説明したデータ転送装置（ＤＴＤ）認証手順を使用するように現在のセルラ電話をアップグレードすることによって行うことができる。認証ソフトウェア・コード及び公衆キーの両方を現存するフラッシュ・メモリに記憶し、このようにして現在の慣例設計ｎに対する何らの変化も回避する。

本発明の模範的応用を、セルラ電話内の電子メモリの安全を保証しかつプログラムするに当たって応用される片方向ハッシュ化及びキー暗号化システムの説明の中で述べた。しかしながら、当業者が容易に承知しかつ認めるように、メモリ

内容のシグネチャを導出するためのいかなる適当な機能、計算、アルゴリズム、方法、及びシステムも本発明に従って応用することができる。また、本発明を特定の実施例を参照して説明した。しかしながら、当業者に容易に明らかなように、上に説明した好適実施例以外の特殊な形で本発明を具体化することが可能である。例えば、本発明をその精神に反することなくいかなる電子メモリ及び／又は電子メモリ・プログラミング又はアクセス装置で具体化することも可能である。更に、本発明をディジタル信号プロセッサ、特定用途向けプロセッサ、又はいかなる他の類似のプロセッサ、又は電子メモリ向けシステムにも応用しかつ実施することがきる。したがって、本明細書に説明した好適実施例は、単に解説のためであって、いずれにしても限定的に考えてはならない。本発明の範囲は、前述の説明によってではなく、添付の請求の範囲によって与えられ、請求の範囲に入る全ての変形実施例及び等価実施例は請求の範囲に包含されることを意図する。

【図１】

Fig.1


B7
C7
B6
M6
B2
C6
C2
M3
B1
M4
M2
C1
M7
M5
B5
B3
M9
C5
C3
M8
B4
M S C
M1
C4
B8
B10
C10
C8
B9
M10
C9

【図２】

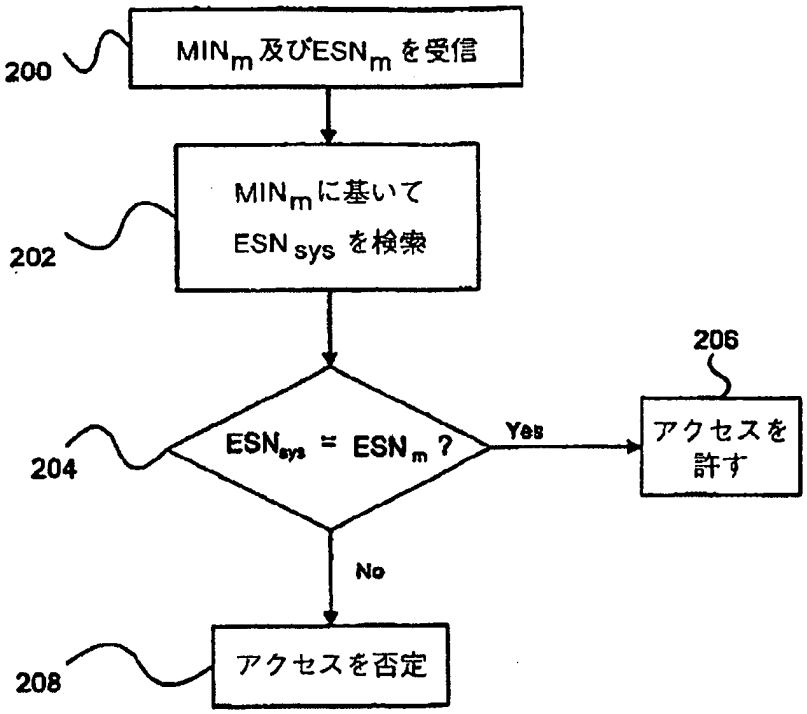

200
MIN$_m$及びESN$_m$を受信
202
MIN$_m$に基いて
ESN$_{sys}$を検索
204
ESN$_{sys}$ = ESN$_m$ ?
Yes
206
アクセスを
許す
No
208
アクセスを否定

Figure 2

【図３】

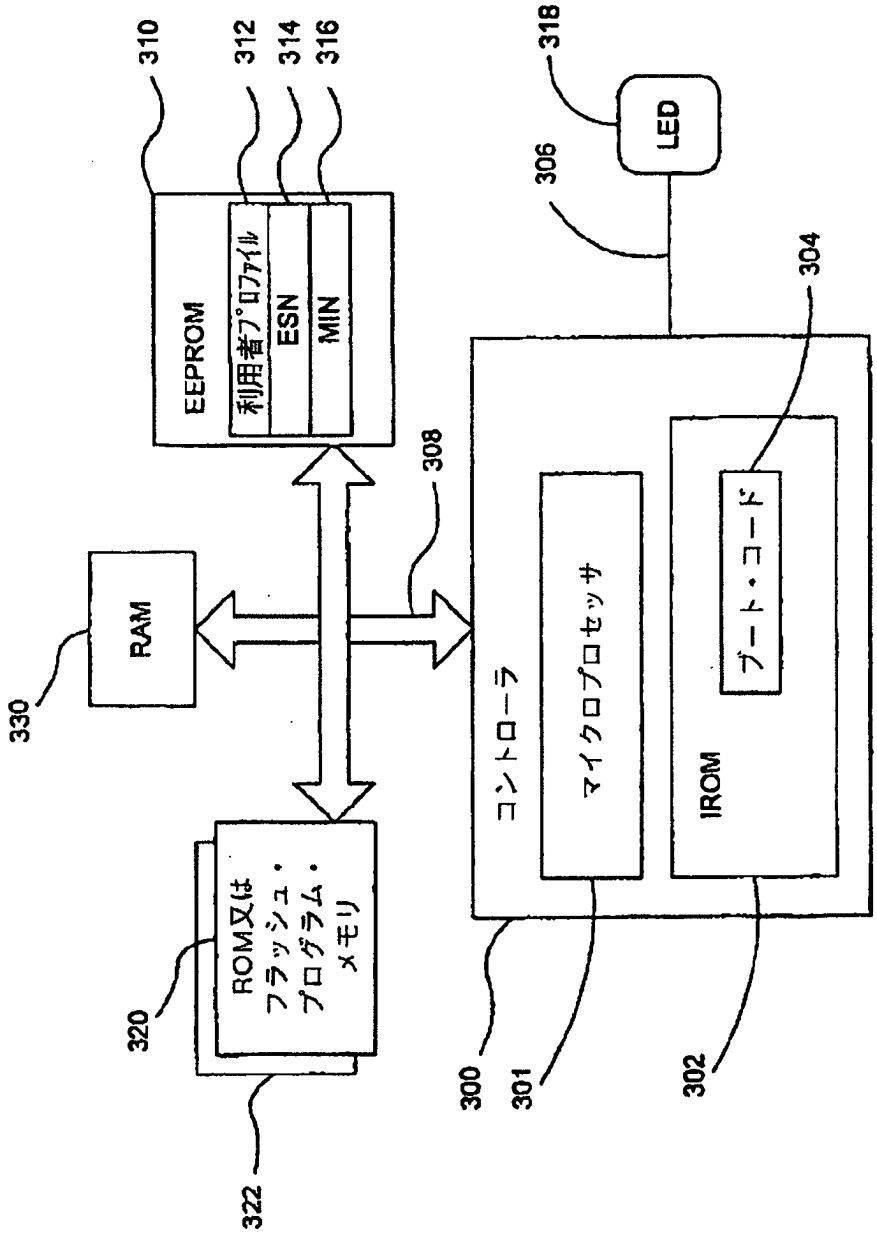

310
312
314
316
318
LED
306
304
EEPROM
利用者ﾌﾟﾛﾌｧｲﾙ
ESN
MIN
308
RAM
330
コントローラ
マイクロプロセッサ
IROM
ブート・コード
ROM又は
フラッシュ・
プログラム・
メモリ
320
322
300
301
302

Figure 3

【図４】

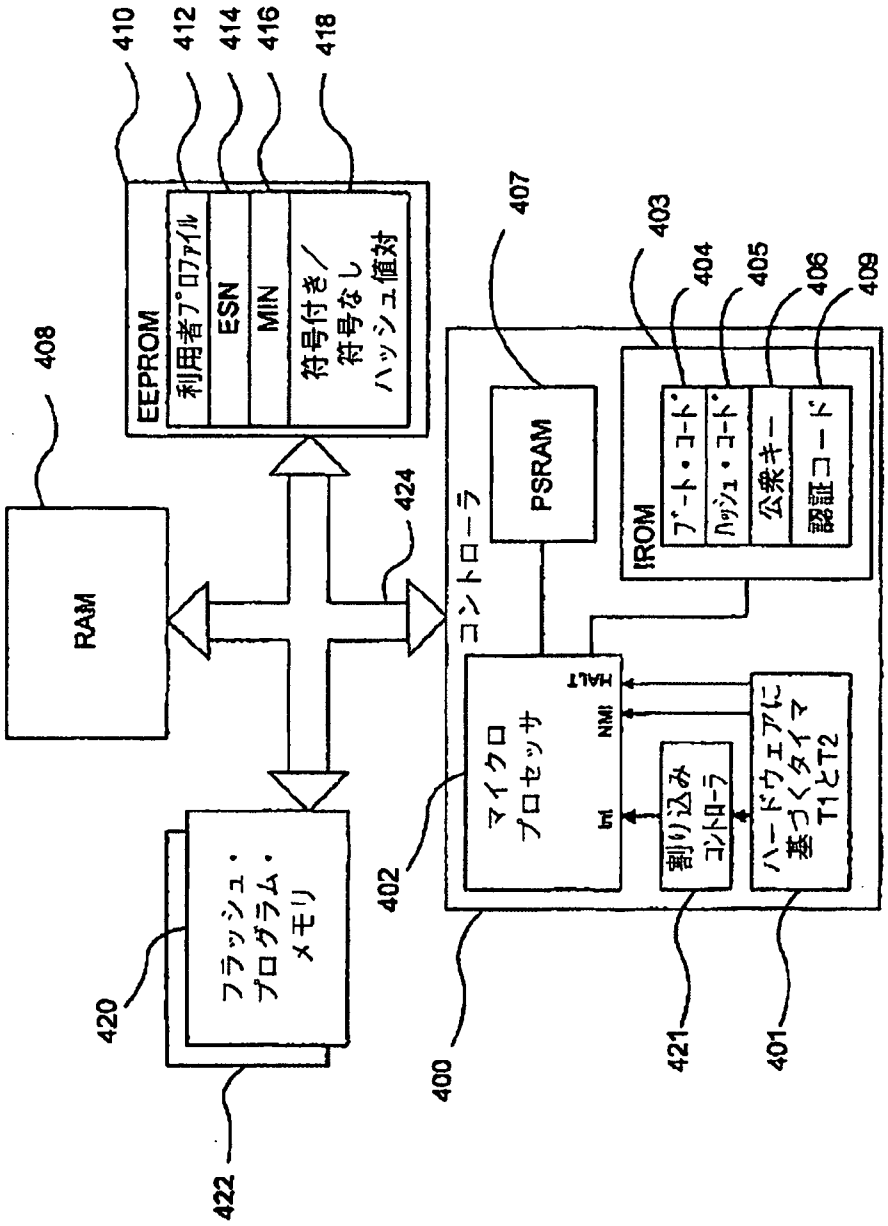

410
412
414
416
418
EEPROM
利用者ﾌﾟﾛﾌｧｲﾙ
ESN
MIN
符号付き／
符号なし
ハッシュ値対
408
RAM
424
407
403
404
405
406
409
コントローラ
PSRAM
IROM
ﾌﾞｰﾄ・ｺｰﾄﾞ
ﾊｯｼｭ・ｺｰﾄﾞ
公衆キー
認証コード
マイクロ
プロセッサ
INT
NMI
HALT
割り込み
コントローラ
ハードウェアに
基づくタイマ
T1とT2
フラッシュ・
プログラム・
メモリ
420
422
402
400
421
401

Figure 4

【図５】

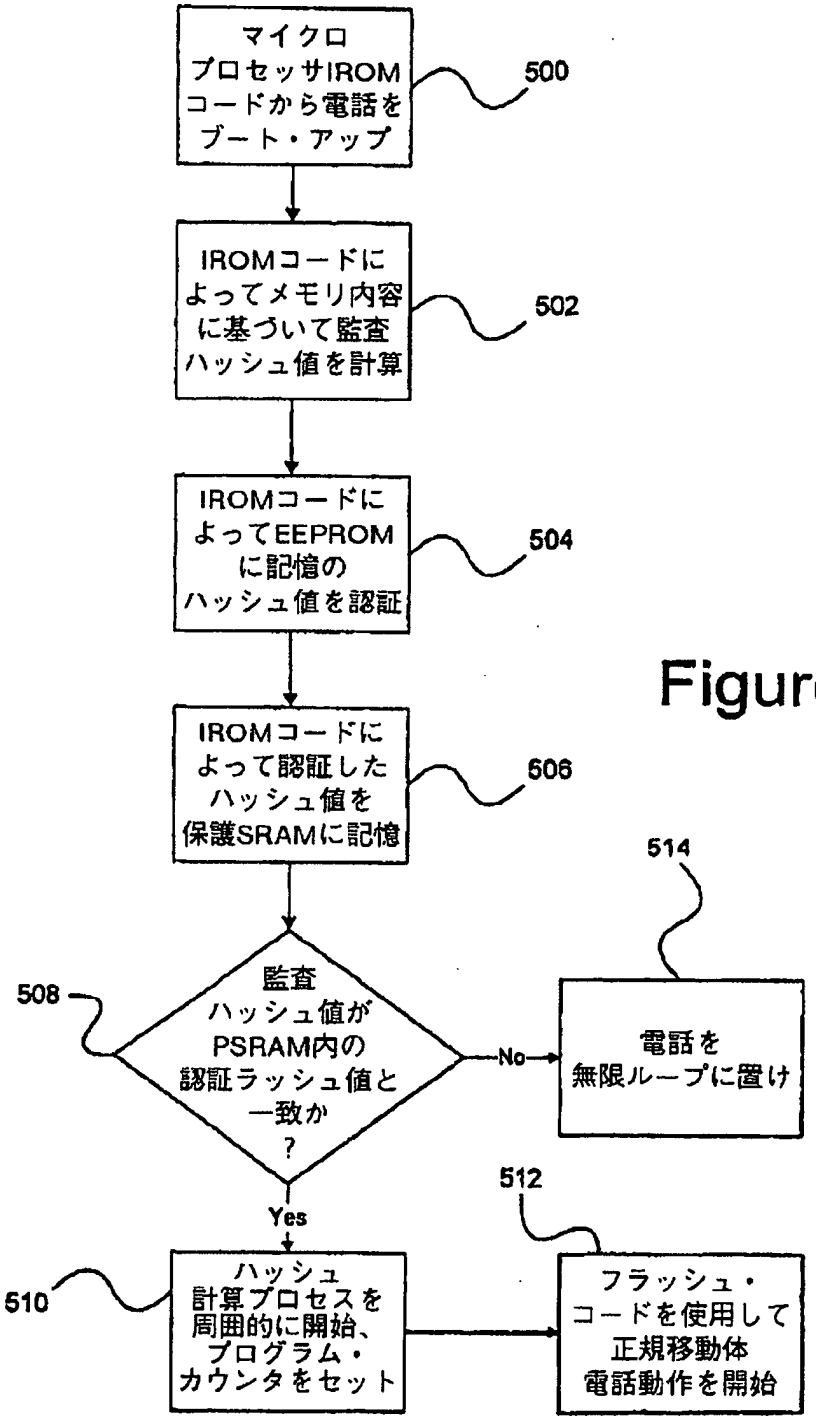

マイクロプロセッサIROMコードから電話をブート・アップ
500
IROMコードによってメモリ内容に基づいて監査ハッシュ値を計算
502
IROMコードによってEEPROMに記憶のハッシュ値を認証
504
IROMコードによって認証したハッシュ値を保護SRAMに記憶
506
514
508
監査ハッシュ値がPSRAM内の認証ラッシュ値と一致か？
No
電話を無限ループに置け
Yes
512
510
ハッシュ計算プロセスを周囲的に開始、プログラム・カウンタをセット
フラッシュ・コードを使用して正規移動体電話動作を開始

Figure 5

【図６】

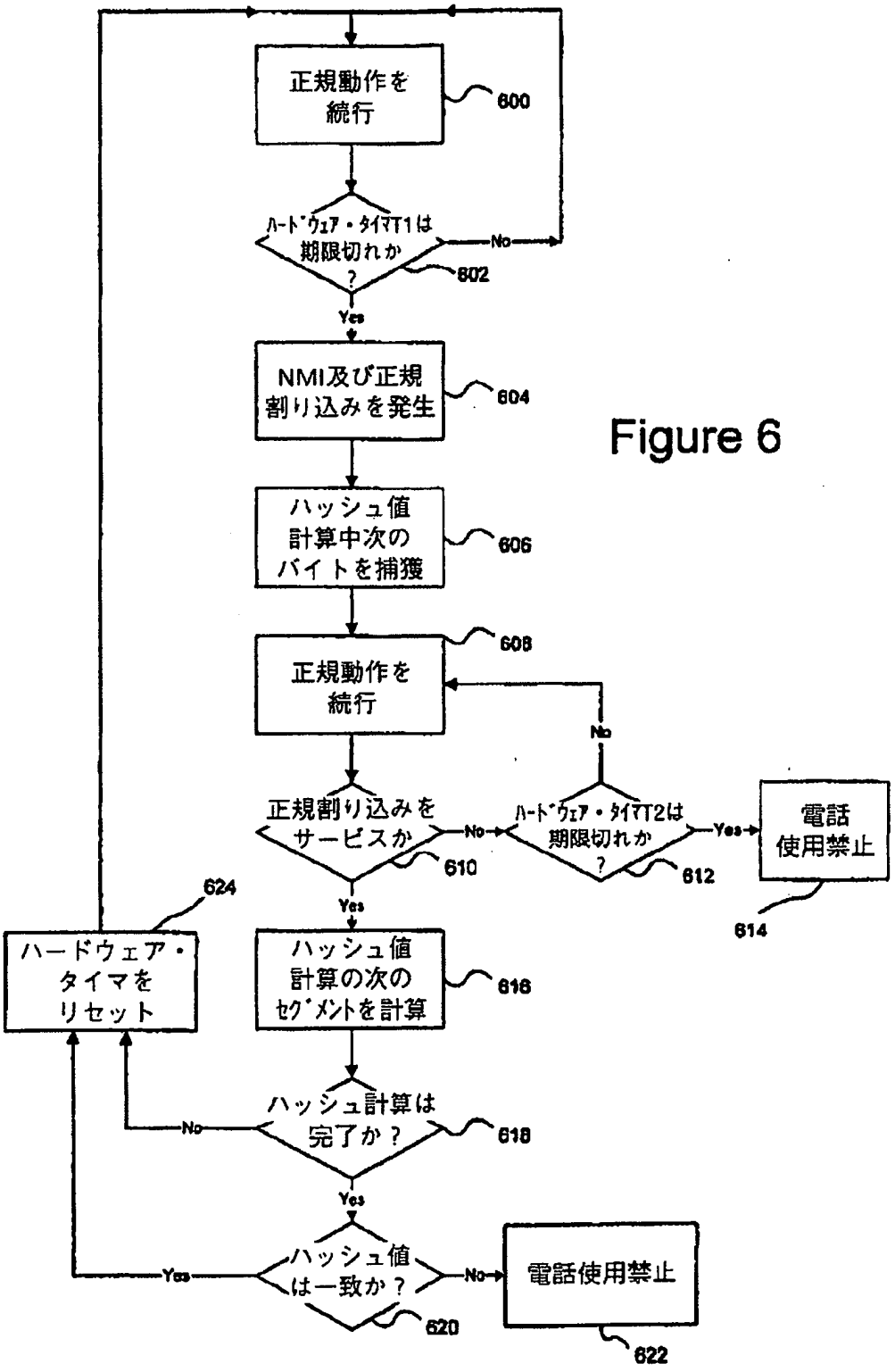

正規動作を
続行
600
ﾊｰﾄﾞｳｪｱ・ﾀｲﾏT1は
期限切れか
？
602
No
Yes
NMI及び正規
割り込みを発生
604
ハッシュ値
計算中次の
バイトを捕獲
606
608
正規動作を
続行
No
正規割り込みを
サービスか
610
No
ﾊｰﾄﾞｳｪｱ・ﾀｲﾏT2は
期限切れか
？
612
Yes
電話
使用禁止
614
Yes
624
ハードウェア・
タイマを
リセット
ハッシュ値
計算の次の
ｾｸﾞﾒﾝﾄを計算
616
ハッシュ計算は
完了か？
618
No
Yes
ハッシュ値
は一致か？
620
Yes
No
電話使用禁止
622

Figure 6

【図７】

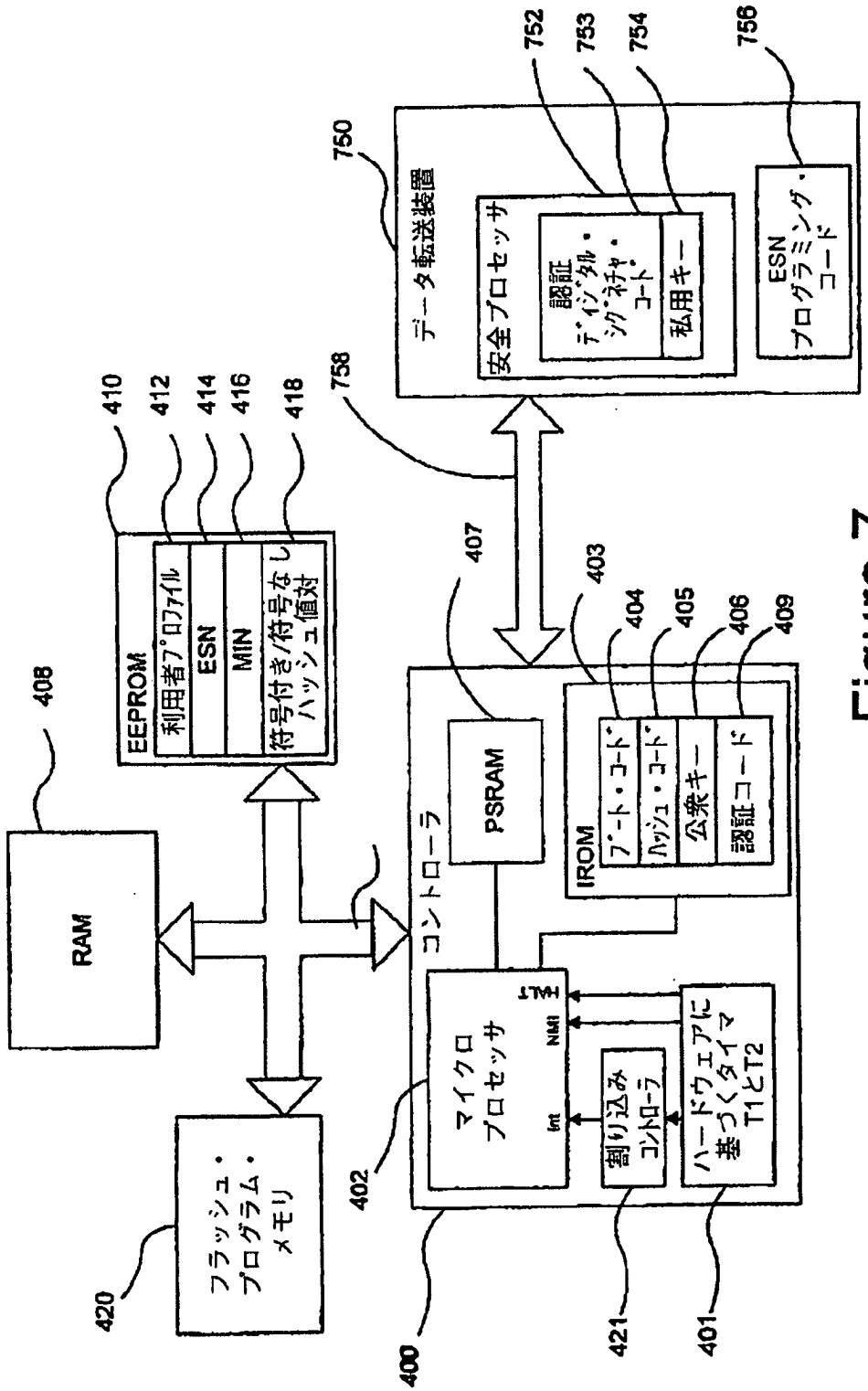

750
データ転送装置
752
753
754
756
安全プロセッサ
認証
ディジタル・シグネチャ・コード
私用キー
ESN
プログラミング・コード
758
410
412
414
416
418
EEPROM
利用者プロファイル
ESN
MIN
符号付き/符号なしハッシュ値対
408
RAM
407
403
404
405
406
409
PSRAM
IROM
ブート・コード
ハッシュ・コード
公衆キー
認証コード
コントローラ
マイクロプロセッサ
NMI
Int
割り込みコントローラ
ハードウェアに基づくタイマT1とT2
フラッシュ・プログラム・メモリ
420
402
400
421
401

Figure 7

【図８】

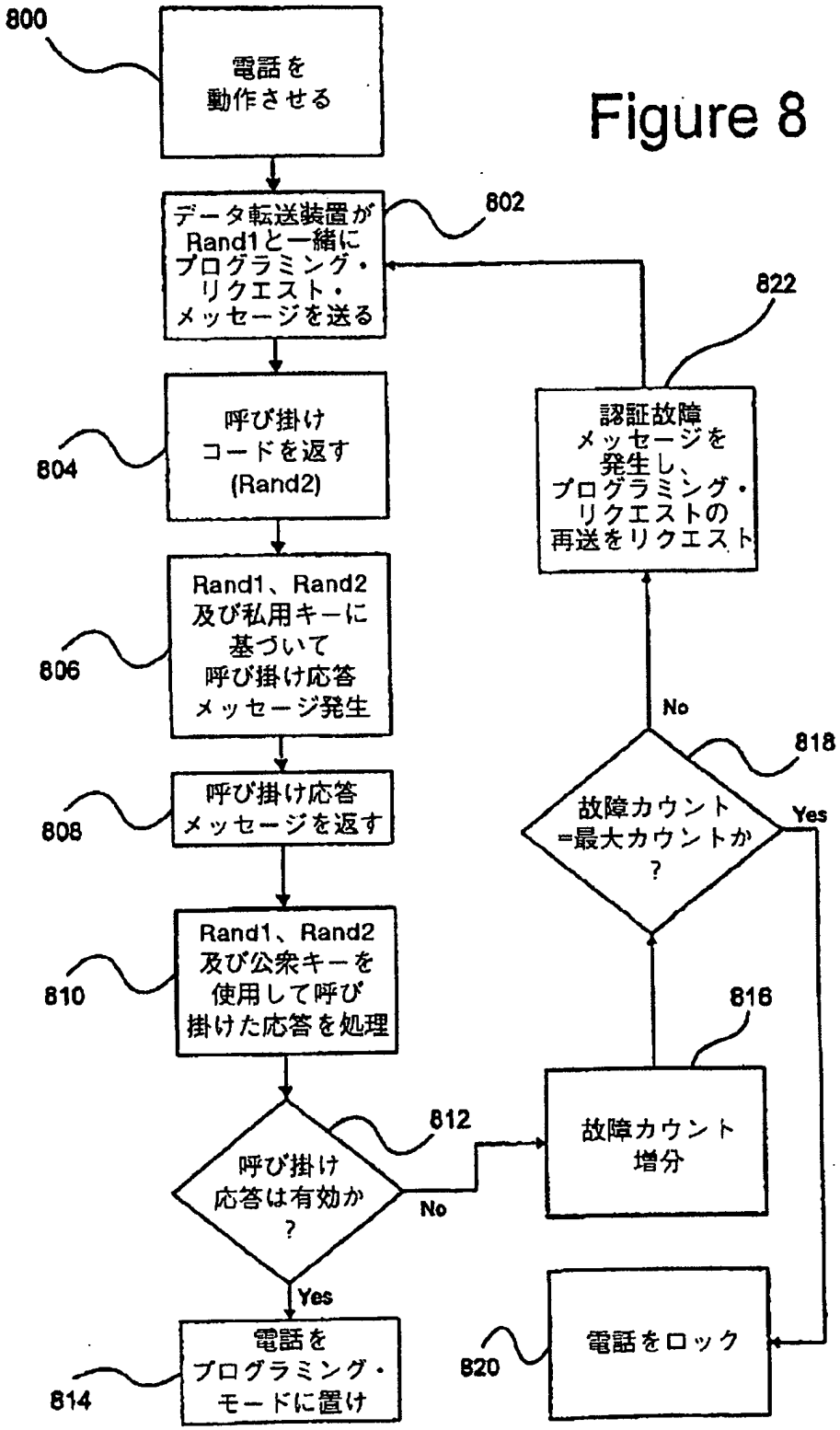

800
電話を動作させる
802
データ転送装置がRand1と一緒にプログラミング・リクエスト・メッセージを送る
804
呼び掛けコードを返す(Rand2)
806
Rand1、Rand2及び私用キーに基づいて呼び掛け応答メッセージ発生
808
呼び掛け応答メッセージを返す
810
Rand1、Rand2及び公衆キーを使用して呼び掛けた応答を処理
812
呼び掛け応答は有効か？
No
Yes
814
電話をプログラミング・モードに置け
816
故障カウント増分
818
故障カウント=最大カウントか？
No
Yes
820
電話をロック
822
認証故障メッセージを発生し、プログラミング・リクエストの再送をリクエスト

Figure 8

【図９】

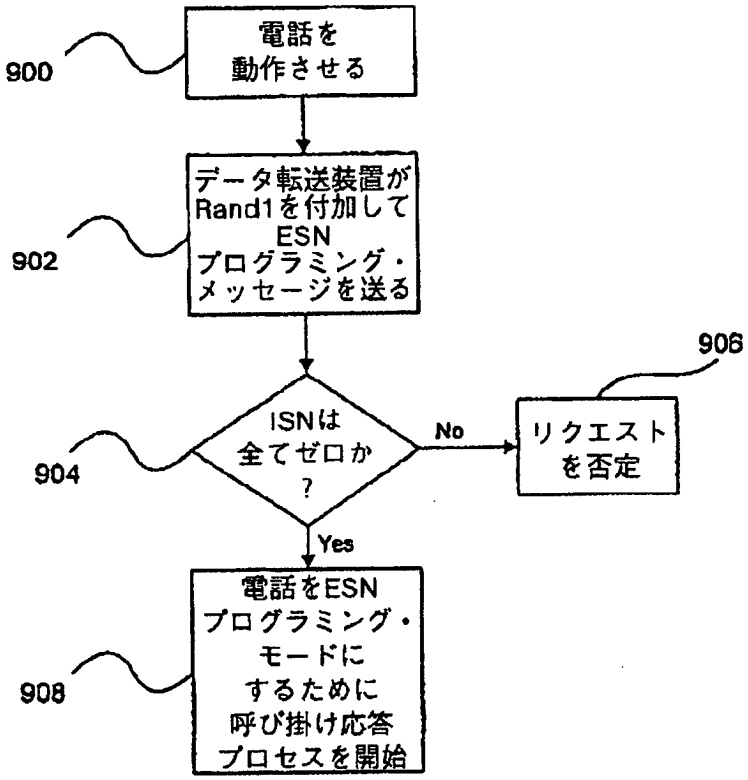
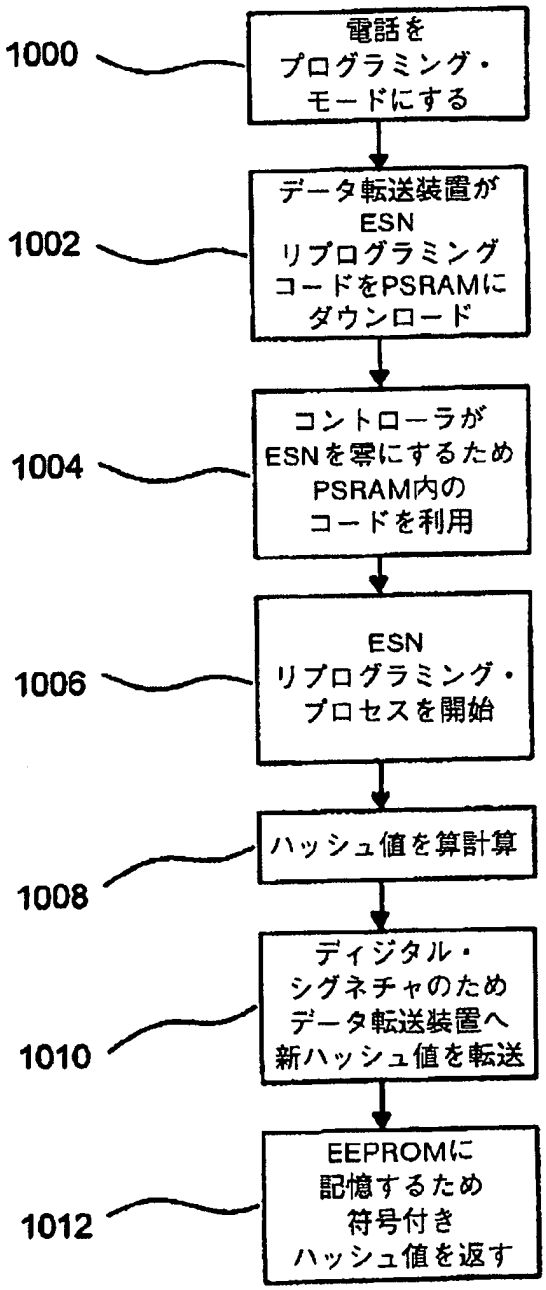

900
電話を
動作させる
902
データ転送装置が
Rand1を付加して
ESN
プログラミング・
メッセージを送る
904
ISNは
全てゼロか
?
No
906
リクエスト
を否定
Yes
908
電話をESN
プログラミング・
モードに
するために
呼び掛け応答
プロセスを開始

Figure 9

【図１０】

FIG. 10


1000
電話を
プログラミング・
モードにする
1002
データ転送装置が
ESN
リプログラミング
コードをPSRAMに
ダウンロード
1004
コントローラが
ESNを零にするため
PSRAM内の
コードを利用
1006
ESN
リプログラミング・
プロセスを開始
1008
ハッシュ値を算計算
1010
ディジタル・
シグネチャのため
データ転送装置へ
新ハッシュ値を転送
1012
EEPROMに
記憶するため
符号付き
ハッシュ値を返す

【図１１】

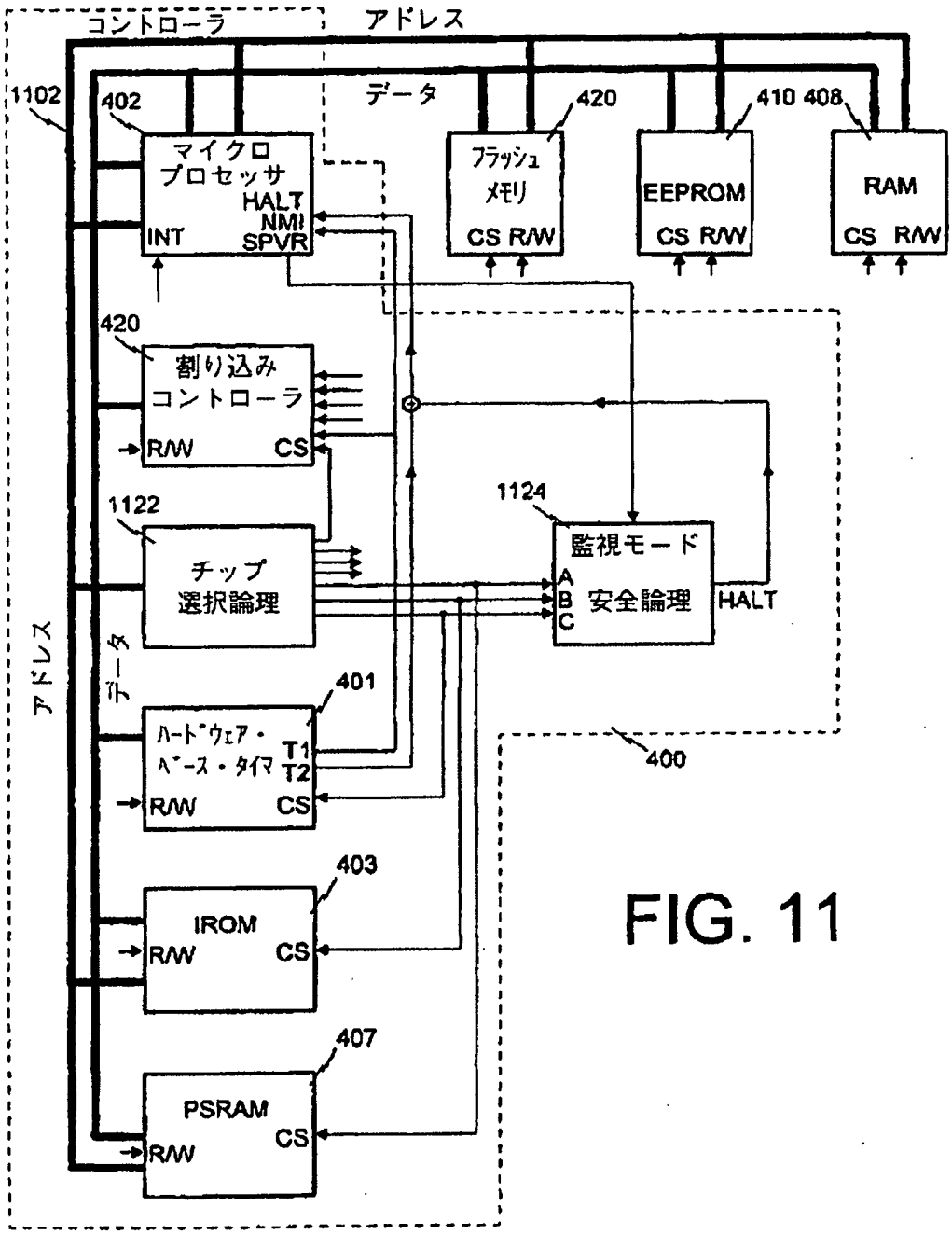

コントローラ
アドレス
データ
1102
402
420
410 408
マイクロ
プロセッサ
HALT
NMI
INT
SPVR
フラッシュ
メモリ
CS R/W
EEPROM
CS R/W
RAM
CS R/W
420
割り込み
コントローラ
R/W
CS
1122
チップ
選択論理
1124
監視モード
A
B
C
安全論理
HALT
アドレス
データ
401
ハードウェア・
ベース・タイマ
T1
T2
R/W
CS
400
403
IROM
R/W
CS
407
PSRAM
CS
R/W

FIG. 11

【図１２】

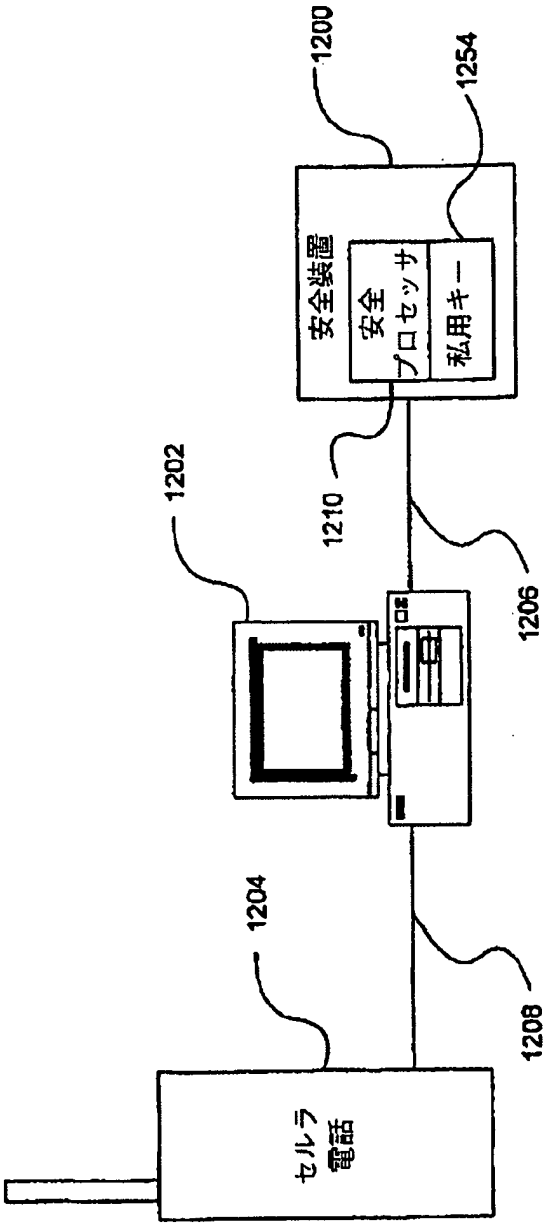



Figure 12

【手続補正書】特許法第１８４条の８第１項

【提出日】平成１０年１２月１５日（１９９８．１２．１５）

【補正内容】

ＥＳＮは、典型的に、移動体電話製造業者によってセットされる。

例えば、アドバンスト・モビール・ホーン・システム（Ａｄｖａｎｃｅｄ Ｍｏｂｉｌｅ Ｐｈｏｎｅ Ｓｙｓｔｅｍ；ＡＭＰＳ）で通信を設定する（ｓｅｔｔｉｎｇ ｕｐ）に当たって利用される慣例の認証方法は、図２に描いた流れ図によって示される。この方法に従って、ブロック２００で、基地局は、移動体電話からのＥＳＮ及びＭＩＮの両方を受信する。これらの認証コードは、それらのコードが移動体電話から受信されることを表示するために、$ESN_m$及び$MIN_m$で指定される。次に、ブロック２０２で、基地局は、システム・メモリから$MIN_m$に対応する$ESN_{sys}$を検索する。次いで、ブロック２０４で、$ESN_{sys}$が$ESN_m$と比較される。もしこれら２つのシリアル番号が同じであるならば、流れ図はブロック２０６へ進み、かつシステム・アクセスが許される。そうでなければ、システム・アクセスは、ブロック２０８で否定される。

詐欺による使用を防止する他の技術が提案されている。例えば、米国特許第５，３８６，４８６号は、サービス通信事業者（ｓｅｒｖｉｃｅ ｃａｒｒｉｅｒ）との専用通信端末に識別番号を登録する方法を説明している。ＥＰ ０ ５８３ １００ Ａ１は、携帯電話内の番号割り当てモジュールの違法設定を防止する携帯電話機用番号割り当てモジュール設定システムを説明している。

このシステムの１つの欠点は、エア・インタフェース上で又は他の発信源から盗聴することによって有効ＭＩＮ／ＥＳＮを組み合わせることが詐欺利用者にとって比較的簡単であることである。もし移動体電話から受信されたＭＩＮ及びＥＳＮがシステム・メモリに記憶されたものに相当するならばこの従来のシステムによるアクセスは有効であると推定されるから、詐欺アクセスにとって必要な情報の全ては、電子盗聴によって得ることができる。

欧州ＧＳＭ規格（移動体通信用グローバル・システム（Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎ；ＧＳＭ））、米国ＴＩＡ／ＥＩＡ／ＩＳ－１３６、及び日本パーソナル・ディジタル・セルラ規

格無線通信システムの下で動作するシステムでは、盗聴から生じる詐欺は呼び掛け応答（ｃｈａｌｌｅｎｇｅ－ｒｅｓｐｏｎｓｅ）方法によって防止される。呼び掛け応答方法に従って、各移動体電話は、その移動体電話及び網内

のデータベースの両方に記憶されている固有の秘密キーと関連している。システムに固有であるアルゴリズムが各移動体電話及び所望の網ノードに記憶される。呼が設定されると、認証がリクエストされ、それによって網が呼び掛け（乱数）を移動体電話へ送る。受信した呼び掛け及び記憶した秘密キーに基づいて、移動体電話は、そのアルゴリズムを使用して応答を計算し、その応答を網へ送信する。同時に、網は「同じ呼び掛け及び網記憶秘密キーに基づいて「期待」応答を計算する。次いで、網は移動体電話の計算した応答を受信し、移動体電話の計算した応答を網の計算した応答と比較する。

典型的最新セルラ電話に含まれたフラッシュ・メモリ３２０は、５１２Ｋのアドレス指定可能容量を有する。偽造者は、フラッシュ・メモリ３２０を除去し、かつ、元のフラッシュ・メモリの内容を１０２４Ｋシャドウ・メモリ３２２の初めの５１２Ｋ内へ複写した後、元のフラッシュ・メモリ３２０を１０２４Ｋシャドウ・メモリで置換することもできる。ブートアップ中、プログラム・メモリへのどのアクセスもフラッシュ・メモリ３２０の初めの５１２Ｋに成功裡に向けられる。次いで、偽造者は、将来の全てのプログラム・メモリ・アクセスをシャドウ・メモリ３２２へスイッチさせるために、ブート・プロセスが完了したことを表示する（ＬＥＤ信号３０６のような）電話内で利用可能な信号を監視することもできる。その後、セルラ電話は、シャドウ・メモリ３２２内にある命令に従って動作し、このメモリをタンブリング・ルーチン・コード及び相当するＭＩＮ／ＥＳＮ対を含むようにプログラムすることができる。

メモリいたずらを防止するために種々の企図がなされてきた。例えば、ＷＯ９１／０９４８４は、移動体無線電話内のメモリ領域へのアクセスがＲＯＭから取り出されたＣＰＵ命令によってのみ許される安全技術を説明している。ＦＲ２６８１　９６５は、或る種の事象の生起の際にメモリが書き込まれるのを防ぐシ

ステムを説明している。詐欺による使用及び／又はいたずらを防止する他のシステムが米国特許第５，０４６，０８２号に記載されており、これはセルラ電話プログラミングに対する無許可アクセス及びいたずらを妨げるセルラ電話用遠隔アクセシング・システムを説明しおり、及び第５，４４２，６４５号はプログラム又はデータの完全性を検査することを説明しており、この検査では携帯物体の処理回路によって計算されたシグネチャが元のメッセージ・シグネチャと比較される。

ほとんどのセルラ詐欺が或る程度のメモリ操作に基づいている理由から、連邦通信委員会（ＦＣＣ）は、セルラ電話詐欺のこの態様に対する解決を現在考え中である。この解決は、第２２．２１９章に示されたＦＣＣ規則案に組み込まれている。現在書かれているように、第２２．９１９章は、移動体電話の動作ソフトウェアが変更可能であることを禁止し、ＥＳＮが工場セットされて、いかなる方法でも変更、転送、除去又は操作されることが不可能であるように要求し、かつ

移動体送信機が、もし製造業者を含むなんらかの者がセルラ電話のＥＳＮ、システム論理、又はファームウェアを除去、いたずら、又は変化させようと企図するならば、動作不可能となることを要求する。

消費者の立場からは、現在の製造業者又はその工場が許可したサービス代理人の現在のセルラ電話をプログラムする能力は、適正に動作しないセルラ電話の置換を容易にしている。例えば、もし加入者のセルラ電話が適正に動作しないならば、その加入者は工場が許可した代理人から新装置を得かつそれを旧装置のものと同じ電子的な「個性（ｐｅｒｓｏｎａｌｉｔｙ）」を含むようにプログラムしてもらうことができる。セルラ電話の電子個性は、ＥＳＮだけでなく、利用者プロファイル及び個人及び／又は業務電話番号のような加入者によってその装置にプログラムされるかなりの量の情報もまた含む。修繕／置換プログラム及びセルラ電話にＥＳＮの変更及び他のメモリの変更を敏速かつ容易に加える技術は、欠陥端末によって自分達の加入者に不便をかけたくないセルラ・サービス提供業者達の主張で開発されてきた。

本発明の範囲は、前述の説明によってではなく、添付の請求の範囲によって与えられる。

## 請求の範囲

１．　電子装置であって、

メモリ（４１０、４２０）と、

認証されたメモリ内容に基づいてハッシュ計算を遂行して有効ハッシュ値を発生し、前記メモリ（４１０、４２０）の内容についてハッシュ計算を遂行して検査ハッシュ値を発生し、前記検査ハッシュ値を前記有効ハッシュ値と比較するマイクロプロセッサ（４０２）あって、前記ハッシュ計算と前記比較が改竄に対して安全である前記マイクロプロセッサ（４０２）と

を含む電子装置。

２．　請求項１記載の電子装置において、前記マイクロプロセッサ（４０２）が、周期的に前記検査ハッシュ値を導出しかつ前記検査ハッシュ値を前記有効ハッシュ値と比較する手段を含む、電子装置。

３．　請求項２記載の電子装置において、前記マイクロプロセッサ（４０２）が、ハードウェアに基づくタイマの期限切れに従って周期的に前記ハッシュ値を導出する手段を含む、電子装置。

４．　請求項１記載の電子装置において、前記メモリが、フラシュ・メモリ（４２０）とＥＥＰＲＯＭ（４１０）とを含む、電子装置。

５．　請求項１記載の電子装置であって、

前記マイクロプロセッサ（４０２）と連携して前記ハッシュ計算を遂する保護されたランダム・アクセス・メモリ（４０７）

を更に含む電子装置。

６．　請求項４記載の電子装置において、前記マイクロプロセッサが、前記フラッシュ・メモリ（４２０）と前記ＥＥＰＲＯＭ（４１０）の選択された内容に基づいて前記監査ハッシュ値を導出する手段を含む、電子装置。

７．　請求項６記載の電子装置において、前記選択された内容が電子的なシリアル番号を含む、電子装置。

８．　請求項６記載の電子装置において、前記選択された内容がマイクロプロセッサ・プログラム・コードを含む、電子装置。

９．　請求項１記載の電子装置において、前記マイクロプロセッサ（４０２）が、前記メモリ（４１０、４２０）内に記憶された公衆キーを使用して前記有効ハッシュ値を認証する手段を含む、電子装置。

１０．　請求項１記載の電子装置において、前記マイクロプロセッサ（４０２）が、私用キーを使用して所与のディジタル・シグネチャで前記有効ハッシュ値を暗号化する手段を含む、電子装置。

１１．　請求項１記載の電子装置において、前記マイクロプロセッサ（４０２）が、Ｓｎｅｒｆｕと、Ｈ－Ｈａｓｈと、ＭＤ２と、ＭＤ４と、ＭＤ５と、Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ（ＳＨＡ）と、ＨＡＶＡＬとを含むハッシュ関数の群のうちの１つを使用して前記ハッシュ計算を遂行する手段を含む、電子装置。

１２．　請求項１記載の電子装置において、前記マイクロプロセッサ（４０２）が、ＥＬＧＡＭＡＬと、ＲＳＡと、ＤＳＡと、フィージ・フィアット・シャミアと、フィアット・シャミアとを含む公衆／私用キー・システム・アルゴリズムの群うちの１つを使用して認証しかつ暗号化する手段を含む電子装置。

１３．　請求項５記載の電子装置であって、前記保護されたランダム・アクセス・メモリへのアクセスを監視する安全論理を更に含む、電子装置。

１４．　請求項１記載の電子装置であって、前記電子装置がセルラ電話である、電子装置。

１５．　請求項６記載の電子装置において、前記フラッシュ・メモリの内容が前記電子装置に対する動作命令を含み、前記ＥＥＰＲＯＭの内容が有効ハッシュ値を含み、前記マイクロプロセッサが有効ハッシュ値を発生するために認証されたフラッシュ内容の選択された部分とＥＥＰＲＯＭ内容の選択された部分とに片方向ハッシュ計算を遂行する手段と、前記選択された部分に前記ハッシュ計算を遂行することによって周期的に検査ハッシュ値を発生する手段と、前記フラッシュ・メモリと前記ＥＥＰＲＯＭメモリの少なくとも１つが変更されたかどうか評

定するために前記検査ハッシュ値を前記認証された有効ハッシュ値と比較する手段とを含む、電子装置。

１６．　請求項１５記載の電子装置において、前記マイクロプロセッサ（４０２）が、Ｓｎｅｒｆｕと、Ｈ－Ｈａｓｈと、ＭＤ２と、ＭＤ４と、ＭＤ５と、Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ（ＳＨＡ）と、ＨＡＶＡＬを含むハッシュ関数の群のうちの１つを使用して片方向ハッシュ計算を遂行する手段を含む、電子装置。

１７．　請求項１０記載の電子装置において、前記マイクロプロセッサ（４０２）が、前記電子装置の外部の処理手段を使用して前記私用キーによるディジタル・シグネチャで前記監査ハッシュ値を暗号化する手段を含む、電子装置。

１８．　電子装置においてメモリ改竄を検出する方法であって、

メモリ（４１０、４２０）の選択された内容にハッシュ計算を遂行することによって発生した符号付き有効ハッシュ値を記憶するステップであって、前記選択されたメモリ内容が認証されている前記記憶するステップと、

前記メモリ（４１０、４２０）の選択された内容に前記ハッシュ計算を遂行することによって検査ハッシュ値を発生するステップと、

前記検査ハッシュ値を前記有効ハッシュ値と比較するステップであって、それによって前記検査ハッシュ値と前記有効ハッシュ値との間の差が前記選択されたメモリ内容の変更を表示する前記比較するステップと

を含み、前記記憶するステップと、前記発生するステップと、前記比較するステップが改竄から安全である方法。

１９．　請求項１８記載の方法において、前記検査ハッシュ値を発生するステップが保護されたランダム・アクセス・メモリ（４０７）と連携して遂行される、方法。

２０．　請求項１８記載の方法であって、

私用キーに基づくディジタル・シグネチャで前記有効ハッシュ値を符号付けするステップ

を更に含む方法。

２１．　請求項１８記載の方法において、前記検査ハッシュ値を発生するステップと、前記検査ハッシュ値を前記有効ハッシュ値と前記比較するステップとが周期的に遂行される、方法。

２２．　請求項１４記載の方法において、前記検査ハッシュ値を発生するステップがハードウェア・ベース・タイマの期限切れに従って遂行される、方法。

２３．　請求項１４記載の方法において、前記検査ハッシュ値を前記発生するステップが検査ハッシュ値セグメントを計算することを伴う、方法。

２４．　請求項２３記載の方法において、前記電子装置内に起こる他のプロセスが完了される間に検査ハッシュ値セグメントの計算を必要なだけ遅延させることができる、方法。

２５．　請求項１８記載の方法において、前記有効ハッシュ値がディジタル・シグネチャを与えられ、及び前記検査ハッシュ値を前記有効ハッシュ値と前記比較するステップが前記シグネチャに対して前記有効ハッシュ値を認証するステップを含む、方法。

２６．　請求項１８記載の方法あって、前記電子装置がセルラ電話である方法。

２７．　メモリ・プログラミング能力を有する電子装置への無許可アクセスを防止するシステムであって、

データ転送装置（７５０）からのアクセス・リクエスト・メッセージに応答して呼び掛け応答認証プロセスを開始させるマイクロプロセッサ（４０２）を含み、前記データ転送装置（７５０）が、私用暗号化キーを使用して前記呼び掛けメッセージを符号付けする手段と、前記電子装置へ前記符号付き呼び掛けメッセージを送る手段とを含み、前記電子装置が、前記私用キーに対応する公衆キーの使用によって前記符号付き呼び掛けメッセージを認証する手段と、前記呼び掛けメッセージが前記認証によって回復されない場合に前記データ転送装置（７５０）を拒否する手段とを更に含む、システム。

２８．　請求項２７記載のシステムであって、前記電子装置がセルラ電話である、システム。

２９．　請求項２８記載のシステムであって、

第１ポートと第２ポートとを有する汎用コンピュータ

をさらに含み、

前記データ転送装置（７５０）が前記第１ポートへの取り付け手段を含み、前記セルラ電話が前記第２ポートへの取り付け手段を含み、前記セルラ電話が前記データ転送装置から受信された前記セルラ電話をプログラムするリクエストに応答して呼び掛けを返す手段を含み、前記呼び掛けが前記データ転送装置によって符号付けされかつ認証のために前記セルラ電話に返され、それによって前記符号付き呼び掛けの認証を通しての前記呼び掛けの回復がデータ転送装置真正を表示しかつ前記セルラ電話をプログラミング・モードにする、

システム。

３０．　メモリ・プログラミング能力を有する電子装置への無許可アクセスを防止する方法であって、

データ転送装置からのアクセス・リクエスト・メッセージに応答して呼び掛けメッセージを送るステップと、

私用暗号化キーを使用して前記データ転送装置（７５０）内で前記呼び掛けメッセージを符号付けするステップと、

前記電子装置（７５０）に前記符号付け呼び掛けメッセージを送るステップと、　公衆キーの使用によって前記電子装置（７５０）内の前記符号付きメッセージを認証するステップであって、前記公衆キーが前記私用暗号化キーに対応する前記認証するステップと、

もし前記呼び掛けメッセージが前記認証するステップによって回復されないならば前記データ転送装置（７５０）を拒否するステップと

を含む方法。

３１．　請求項３０記載の方法あって、前記電子装置がセルラ電話である、方法。

３２．　請求項３０記載の方法あって、前記符号付き呼び掛けメッセーシが前記呼び掛けメッセージの部分に依存する呼び掛け応答メッセージであり、前記符

号付き呼び掛け応答メッセージが前記データ転送装置の真正を確認する場合に認証のプログラミング・モードに入るステップを更に含む方法。

３３．　プログラミング能力を有する電子装置であって、

前記電子装置への無許可アクセスを防止するマイクロプロセッサ（４０２）を含み、前記電子装置がデータ転送装置からの前記電子装置へアクセスするリクエストに応答して前記データ転送装置（７０５）へ呼び掛けメッセージを発する手段を含み、前記データ転送装置が、私用暗号化キーを使用して前記呼び掛けメッセージを符号付けする手段と、前記電子装置へ前記符号付き呼び掛けメッセージを送る手段とを含み、及び前記電子装置が前記私用キーに対応する公衆キーの使用によって前記符号付き呼び掛けメッセージを認証する手段と、前記呼び掛けメッセージが前記認証によって回復されない場合に前記データ転送装置（７５０）を拒否する手段とを更に含む、電子装置。

３４．　請求項３３記載の電子装置あって、前記電子装置がセルラ電話であり、前記データ転送装置がプログラマである、電子装置。

３５．　メモリ・アクセスを防止するシステムであって、

マイクロプロセッサ（４０２）と、

命令コードを含む読み出し専用メモリ（４０３）と、

保護されたランダム・アクセス・メモリ（４０７）と

前記保護されたランダム・アクセス・メモリ（４０７）へアクセスする企図を検出し、前記読み出し専用メモリ（４０３）によるアクセスを許し、かつ、それ以外によるならば、マイクロプロセッサ（４０２）に動作を停止させかつこのようなアクセスを防止させる安全論理（１１２４）と、

を含むシステム。

３６．　請求項３５記載のシステムであって、ハードウェアに基づくタイマ（４０１）を更に含み、前記安全論理（１１２４）が、前記読み出し専用メモリ（４０３）による前記ハードウェア・ベース・タイマ（４０１）へのアクセスを許し、それ以外によるアクセスを防止する、システム。

３７．　請求項３５記載のシステムにおいて、前記読み出し専用メモリ（４０

３）内の命令コードに従う前記保護されたランダム・アクセス・メモリ（４０７）へのアクセスは、前記システムが監視モードにあるときに限り起こり得る、システム。

３８．　請求項３５記載のシステムであって、セルラ電話におけるメモリアクセスを防止するシステム。

【国際調査報告】

# INTERNATIONAL SEARCH REPORT

Ins. ional Application No
PCT/US 97/15311

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| | -/-- | |

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 29 April 1998 | 18. 05. 98 |
| Name and mailing address of the ISA<br>European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Authorized officer<br>Gerling, J.C.J. |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Int ational Application No
PCT/US 97/15311

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X<br>Y<br>A | US 5 046 082 A (ZICKER ROBERT G ET AL) 3 September 1991<br>see column 3, line 26 - line 29<br>see column 3, line 46 - line 49<br>see column 4, line 11 - line 18<br>see column 7, line 43 - line 57<br>see column 8, line 20 - line 22<br>see column 8, line 35 - line 54<br>see column 11, line 67 - column 12, line 4<br>see column 12, line 9 - line 33<br>see column 14, line 17 - line 22<br>see column 16, line 27 - line 48<br>see column 17, line 13 - line 16<br>see column 17, line 58 - column 18, line 33<br>see column 18, line 3 - line 50<br>see column 20, line 35 - line 42<br>see column 23, line 10 - line 12<br>see column 27, line 43 - column 28, line 21; figures 8,9 | 27-30,<br>32,51<br>1,14,22<br>2-4,6-8,<br>10,15-18 |
| X<br>Y | US 5 442 645 A (UGON MICHEL ET AL) 15 August 1995<br>see column 2, line 51 - column 3, line 11<br>see column 3, line 50 - line 57<br>see column 4, line 50 - line 57<br>see column 5, line 1 - line 7<br>see column 5, line 46 - line 54<br>see column 6, line 5 - column 7, line 17<br>see column 7, line 43 - line 46<br>see column 8, line 6 - line 14<br>see column 8, line 49 - line 61<br>see column 9, line 30 - line 45<br>see column 14, line 63 - column 15, line 50<br>see claim 1 | 36,42,<br>45,46,<br>48-50<br>1,14,22 |
| X<br>Y | EP 0 583 100 A (NIPPON ELECTRIC CO)<br>see column 4, line 48 - column 5, line 27; figures 1,2<br>see column 3, line 35 - column 4, line 3<br>see column 2, line 30 - column 3, line 8 | 27,51<br>28-32 |
| A | PRENEEL B: "CRYPTOGRAPHIC HASH FUNCTIONS" EUROPEAN TRANSACTIONS ON TELECOMMUNICATIONS AND RELATED TECHNOLOGIES, vol. 5, no. 4, July 1994, pages 17-34, XP000460559<br>see page 29, left-hand column, paragraph 5.4. - right-hand column, paragraph 6. | 1,14,22,<br>36,45 |

-/--

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/US 97/15311

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 5 386 468 A (AKIYAMA RYOTA ET AL) 31 January 1995 | 28-32 |
| A | see column 2, line 60 - line 68<br>see column 3, line 23 - line 35<br>see column 3, line 43 - column 4, line 7 | 1,14,22, 36,45 |
| A | US 5 400 389 A (NIIYAMA MANABU ET AL) 21 March 1995<br>see column 3, line 60 - line 64<br>see column 4, line 6 - line 12; figures 1,2 | 1,14,22, 36,45 |
| X | WO 91 09484 A (CETELCO AS)<br>see page 10, line 29 - page 11, line 27<br>see page 8, line 28 - page 9, line 6 | 33,35, 52,54 |
| Y | see page 4, line 7 - page 6, line 8 | 34,53 |
| Y | FR 2 681 965 A (MOTOROLA INC)<br>see page 4, line 35 - page 5, line 6<br>see page 3, line 3 - line 10<br>see page 2, line 17 - line 25 | 34,53 |

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

## INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 97/15311

**Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)**

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (1)) (July 1992)

International Application No. PCT/US 97/15311

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

1. Claims: 1-26,36-50

DETECTING TAMPERING WITH AN ELECTRONIC MEMORY.

2. Claims: 27-32,51

AUTHENTICATION OF A REPROGRAMMING REQUEST. see annex

3. Claims: 33-35,52-54

SECURITY LOGIC FOR PROTECTED MEMORY

see annex

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. Jonal Application No
PCT/US 97/15311

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 5046082 A | 03-09-91 | NONE | |
| US 5442645 A | 15-08-95 | FR 2647924 A | 07-12-90 |
| | | AT 127252 T | 15-09-95 |
| | | CA 2034002 A,C | 07-12-90 |
| | | DE 69021935 D | 05-10-95 |
| | | DE 69021935 T | 15-02-96 |
| | | EP 0402210 A | 12-12-90 |
| | | ES 2079457 T | 16-01-96 |
| | | WO 9015384 A | 13-12-90 |
| | | HK 80897 A | 20-06-97 |
| | | JP 7027497 B | 29-03-95 |
| | | JP 3503220 T | 18-07-91 |
| | | KR 9409699 B | 17-10-94 |
| EP 0583100 A | 16-02-94 | JP 6053900 A | 25-02-94 |
| | | US 5414753 A | 09-05-95 |
| US 5386468 A | 31-01-95 | JP 6097931 A | 08-04-94 |
| US 5400389 A | 21-03-95 | JP 5327582 A | 10-12-93 |
| WO 9109484 A | 27-06-91 | DK 624489 A | 12-06-91 |
| | | AU 7038391 A | 18-07-91 |
| FR 2681965 A | 02-04-93 | CA 2097308 A | 02-04-93 |
| | | IT 1258856 B | 01-03-96 |
| | | MX 9205634 A | 01-04-93 |
| | | WO 9307565 A | 15-04-93 |

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(GH, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成17年5月12日(2005.5.12)

【公表番号】特表2001-500293(P2001-500293A)
【公表日】平成13年1月9日(2001.1.9)
【出願番号】特願平10-512770
【国際特許分類第７版】
　Ｇ０６Ｆ　12/14
　Ｇ０９Ｃ　 1/00
　Ｈ０４Ｌ　 9/32
　Ｈ０４Ｑ　 7/38
【ＦＩ】
　Ｇ０６Ｆ　12/14　　３１０Ｚ
　Ｇ０９Ｃ　 1/00　　６４０Ｄ
　Ｈ０４Ｂ　 7/26　　１０９Ｒ
　Ｈ０４Ｌ　 9/00　　６７５Ａ

【手続補正書】
【提出日】平成16年9月1日(2004.9.1)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】補正の内容のとおり
【補正方法】変更
【補正の内容】

# 手　続　補　正　書

適

平成１６年 9月 1日

特許庁長官殿

1. 事件の表示

平成１０年特許願第５１２７７０号

2. 補正をする者

事件との関係　特許出願人

名　称　エリクソン　インコーポレイテッド

3. 代　理　人

居　所　〒100-0004　東京都千代田区大手町二丁目２番１号
新　大　手　町　ビ　ル　ヂ　ン　グ　３　３　１
電　話　（３２１１）３６５１（代表）
氏　名　（６６６９）　浅　村　　皓

4. 補正対象書類名

明　細　書
図　面

5. 補正対象項目名

明　細　書
図　面

6. 補正の内容　別紙のとおり

特許庁 16.9.2 出願令後課 金井

（１）図９を別紙の通り補正する。
（２）明細書第１頁第１０行の「メモリの詐欺」を『メモリの詐欺（不正）』と補正する。
（３）明細書第３頁第１５行の「勘定」を『アカウント』と補正する。
（４）明細書第３頁第２２行の「勘定」を『アカウント』と補正する。
（５）明細書第５頁第１１行の「リプロルグラム」を『リプログラム』と補正する。
（６）明細書第１０頁第１５行の「公衆／私用」を『公衆／私用（Public/Private）と補正する。』
（７）明細書第１０頁第２６行の「メセージ」を『メッセージ』と補正する。
（８）明細書第１２頁第２９行の「フラシュ」を『フラッシュ』と補正する。
（９）明細書第１３頁第１１行の「フラシュ」を『フラッシュ』と補正する。
（１０）明細書第１７頁第１行の「新フラッシュ・メモリ４２０内容」を『新しいフラッシュ・メモリ４２０の内容』と補正する。
（１１）明細書第１７頁第７行の「認証故障」を『認証失敗』と補正する。
（１２）明細書第２２頁第２７行の「平方余剰」を『平方剰余』と補正する。
（１３）明細書第２４頁第９行の「↑Ｓｐｕｒｖ」を『↑Ｓｕｐｒｖ』と補正する。
（１４）明細書第２５頁第２６行の「計ｎに」を『計に』と補正する。
（１５）３４条補正書第１頁の第１３行から第２３行の
「　詐欺による使用を防止する他の技術が提案されている。例えば、米国特許５，３８６，４８６号は、サービス通信事業者（ｓｅｒｖｉｃｅ　ｃａｒｒｉｅｒ）との専用通信端末に識別番号を登録する方法を説明している。ＥＰ　０　５８３　１００　Ａ１は、携帯番号内の番号割り当てモジュールの違法設定を防止する携帯番号機用番号割り当てモジュール設定システムを説明している。

　このシステムの１つの欠点は、エア・インターフェイス上で又は他の発信源から盗聴することによって有効ＭＩＮ／ＥＳＮを組み合わせることが詐欺利用者にとって比較的簡単であることである。もし移動体電話から受信され

たＭＩＮ及びＥＳＮがシステム・メモリに記憶されたものに相当するならばこの従来のシステムによるアクセスは有効であると推定されるから、詐欺アクセスにとって必要な情報の全ては、電子盗聴によって得ることができる。」を

『 このシステムの１つの欠点は、エア・インターフェイス上で又は他の発信源から盗聴することによって有効ＭＩＮ／ＥＳＮを組み合わせることが詐欺利用者にとって比較的簡単であることである。もし移動体電話から受信されたＭＩＮ及びＥＳＮがシステム・メモリに記憶されたものに相当するならばこの従来のシステムによるアクセスは有効であると推定されるから、詐欺アクセスにとって必要な情報の全ては、電子盗聴によって得ることができる。

詐欺による使用を防止する他の技術が提案されている。例えば、米国特許５，３８６，４８６号は、サービス通信事業者（ｓｅｒｖｉｃｅ ｃａｒｒｉｅｒ）との専用通信端末に識別番号を登録する方法を説明している。ＥＰ ０ ５８３ １００ Ａ１は、携帯番号内の番号割り当てモジュールの違法設定を防止する携帯番号機用番号割り当てモジュール設定システムを説明している。』と補正する。

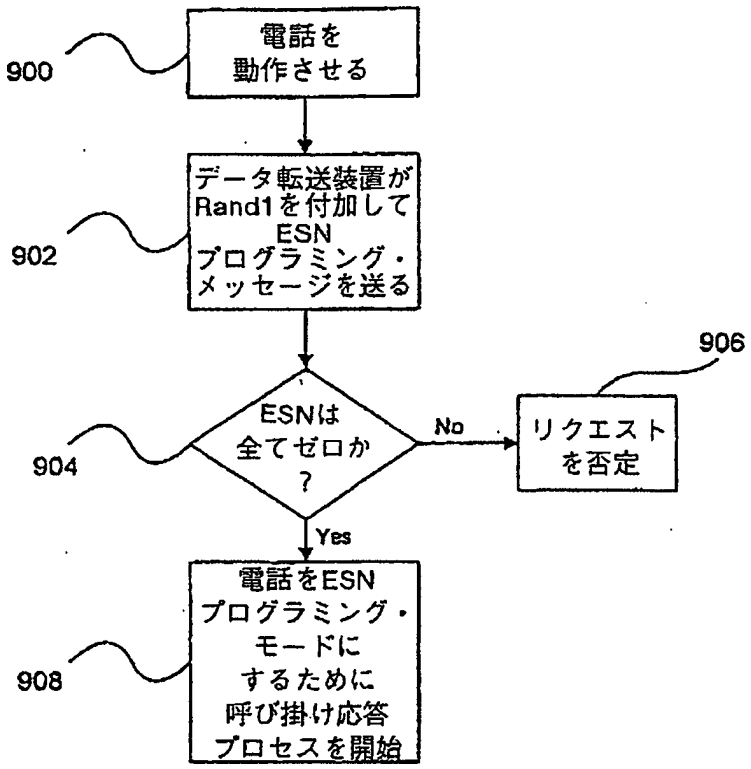

900
電話を
動作させる
902
データ転送装置が
Rand1を付加して
ESN
プログラミング・
メッセージを送る
904
ESNは
全てゼロか
?
No
906
リクエスト
を否定
Yes
908
電話をESN
プログラミング・
モードに
するために
呼び掛け応答
プロセスを開始

Figure 9